SonicWALL ViewPoint User's Guide

Version 2.5

Copyright Information

© 2003 SonicWALL, Inc. All rights reserved.

Under the copyright laws, this manual or the software described within, may not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. Under the law, copying includes translating into another language or format.

SonicWALL is a registered trademark of SonicWALL, Inc.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions subject to change without notice.

Part Number: 232-000369-01 Rev A

Software License Agreement for SonicWALL ViewPoint

This Software License Agreement (SLA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package(s), installing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this SLA. If you do not agree to the terms of this SLA, do not open the sealed package(s), install or use the SOFTWARE PRODUCT. You may however return the unopened SOFTWARE PRODUCT to your place of purchase for a full refund.

The SOFTWARE PRODUCT is licensed, not sold.

You acknowledge and agree that all right, title, and interest in and to the SOFTWARE PRODUCT, including all associated intellectual property rights, are and shall remain with SonicWALL. This SLA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this SLA.

oThe SOFTWARE PRODUCT is licensed as a single product.

oYou may also store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used only to install or run the SOFTWARE PRODUCT on your other computers over an internal network.

oYou may not resell, or otherwise transfer for value, rent, lease, or lend the SOFTWARE PRODUCT.

oThe SOFTWARE PRODUCT is trade secret or confidential information of SonicWALL or its licensors. You shall take appropriate action to protect the confidentiality of the SOFTWARE PRODUCT. You shall not reverse-engineer, de-compile, or disassemble the SOFTWARE PRODUCT, in whole or in part. The provisions of this section will survive the termination of this SLA.

oYou agree and certify that neither the SOFTWARE PRODUCT nor any other technical data received from SonicWALL, nor the direct product thereof, will be exported outside the United States except as permitted by the laws and regulations of the United States, which may require U.S. Government export approval/licensing. Failure to strictly comply with this provision shall automatically invalidate this License.

LICENSE

SonicWALL grants you a non-exclusive license to use the SOFTWARE PRODUCT for a number of SonicWALL Internet Security Appliances. This number is specified and shipped with the SOFTWARE PRODUCT. Support for additional SonicWALL Internet Security Appliances is subject to a separate upgrade license.

OEM - If the SOFTWARE PRODUCT is modified and enhanced for a SonicWALL OEM partner, you must adhere to the software license agreement of the SonicWALL OEM partner.

UPGRADES

If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use a product identified by SonicWALL as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this SLA. If the SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

DISTRIBUTION RIGHTS

To i-net SPRINTA(tm) 2000 DRIVER - SonicWALL has been given a non-exclusive, worldwide license by i-net software GmbH to distribute directly and indirectly (through SonicWALL's distribution channels) the i-net SPRINTA(tm) 2000 driver to SonicWALL's end user customers to use the driver with SonicWALL ViewPoint. SonicWALL's end user customers may make a copy of the driver for backup or archival purposes only. SonicWALL's end user customers are not allowed to make other copies, transfer, re-distribute, use, translate, or reverse assemble/compile the driver with any other non-SonicWALL applications. i-net software GmbH holds copyright and title to the i-net SPRINTA(tm) 2000 Driver.

To Microsoft's SQL Server Developer's Edition (MSDE) - This software incorporates Microsoft's SQL Server Developer's Edition (MSDE) and your use is subject to the terms and conditions of Microsoft's MSDE End-User License Agreement (a copy of which is available on Microsoft's website: <http://www.microsoft.com/sql/howtobuy/deveula.asp>).

To Quest Software's (formerly Sitraka) JClass ServerChart - This software incorporates Quest Software's (formerly Sitraka) JClass ServerChart and your use is subject to the terms and conditions of Quest's Jclass License Agreement (a copy of which is available on Quest's website: <http://java.quest.com/jclass/licensing.shtml>).

SUPPORT SERVICES

SonicWALL may provide you with support services related to the SOFTWARE PRODUCT (“Support Services”). Use of Support Services is governed by the SonicWALL policies and programs described in the user manual, in “online” documentation, and/or in other SonicWALL-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to terms and conditions of this SLA. With respect to technical information you provide to SonicWALL as part of the Support Services, SonicWALL may use such information for its business purposes, including for product support and development. SonicWALL shall not utilize such technical information in a form that identifies its source.

OWNERSHIP

As between the parties, SonicWALL retains all title to, ownership of, and all proprietary rights with respect to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and 'applets” incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is protected by copyrights laws and international treaty provisions. The SOFTWARE PRODUCT is licensed, not sold. This SLA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this SLA.

U.S. GOVERNMENT RESTRICTED RIGHTS

If you are acquiring the Software including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense (“DoD”), the Software is subject to “Restricted Rights”, as that term is defined in the DOD Supplement to the Federal Acquisition Regulations (“DFAR”) in paragraph 252.227 7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government's rights in the Software will be as defined in paragraph 52.227 19(c) (2) of the Federal Acquisition Regulations (“FAR”). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions. Contractor/Manufacturer is: SonicWALL, Inc. 1143 Borregas Avenue, Sunnyvale, California 94089.

MISCELLANEOUS

This SLA represents the entire agreement concerning the subject matter hereof between the parties and supersedes all prior agreements and representations between them. It may be amended only in writing executed by both parties. This SLA shall be governed by and construed under the laws of the State of California as if entirely performed within the State and without regard for conflicts of laws. Should any term of this SLA be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

TERMINATION

This SLA is effective upon your opening of the sealed package(s), installing or otherwise using the SOFTWARE PRODUCT, and shall continue until terminated. Without prejudice to any other rights, SonicWALL may terminate this SLA if you fail to comply with the terms and conditions of this SLA. In such event, you agree to return or destroy the SOFTWARE PRODUCT (including all related documents and components items as defined above) and any and all copies of same.

LIMITED WARRANTY

SonicWALL warrants that a) the software product will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of purchase, and b) any support services provided by SonicWALL shall be substantially as described in applicable written materials provided to you by SonicWALL. Any implied warranties on the software product are limited to ninety (90) days. Some states and jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES

SonicWALL's and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the SOFTWARE PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE PRODUCT has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside of the United States, neither these remedies nor any product Support Services offered by SonicWALL are available without proof of purchase from an authorized SonicWALL international reseller or distributor.

NO OTHER WARRANTIES

To the maximum extent permitted by applicable law, SonicWALL and its suppliers/licensors disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE PRODUCT, and the provision of or failure to provide support services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

LIMITATION OF LIABILITY

Except for the warranties provided hereunder, to the maximum extent permitted by applicable law, in no event shall SonicWALL or its suppliers/licensors be liable for any special, incidental, indirect, or consequential damages for lost business profits, business interruption, loss of business information,) arising out of the use of or inability to use the SOFTWARE PRODUCT or the provision of or failure to provide support services, even if SonicWALL has been advised of the possibility of such damages. In any case,

SonicWALL's entire liability under any provision of this SLA shall be limited to the amount actually paid by you for the SOFTWARE PRODUCT; provided, however, if you have entered into a SonicWALL support services agreement, SonicWALL's entire liability regarding support services shall be governed by the terms of that agreement. Because some states and jurisdiction do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

Manufacturer is SonicWALL, Inc. with headquarters located at 1143 Borregas Avenue, Sunnyvale, CA 94089, USA.

CONTENTS

Preface About this Book 11

Audience 12
Related Publications 12
Document Organization 12
Document Conventions 12
Visual Conventions 13
Text Conventions 13
Additional Help 14

Chapter 1 Introducing SonicWALL ViewPoint 15

Key Features & Benefits 16

Chapter 2 Installing SonicWALL ViewPoint 19

System Requirements 20
Installation 20
Registering ViewPoint 25
Creating a mysonicwall.com Account 25
Registering a SonicWALL Appliance 25
Activating Your ViewPoint Software 26
Enabling the ViewPoint License 27

Chapter 3 Configuring ViewPoint 29

Logging Into ViewPoint 30
Configuring a SonicWALL Appliance for ViewPoint 31
Configuring Access to a SonicWALL Appliance 33
Adding a SonicWALL Appliance to ViewPoint 35
Viewing and Updating SonicWALL Information 37
Deleting a SonicWALL Appliance from ViewPoint 38
Modifying Settings for a SonicWALL Appliance 39
Changing Your ViewPoint Login Password 40
Configuring ViewPoint Settings 41
Viewing and Managing ViewPoint Logs 42

Managing ViewPoint Sessions 43
Configuring E-mail and Alert Settings 44
Summarizer Settings 46
General Report Settings 46
Configuring Log Viewer Settings 47
Configuring Email/Archive Settings 48
Adding a Service 50

Chapter 4 Scheduling ViewPoint Reporting 51
Scheduling a Daily Report 52
Scheduling a Weekly or Monthly Report 53

Chapter 5 Viewing Reports 55
Viewing Bandwidth Reports 55
Viewing the Bandwidth Summary Report 56
Monitoring Bandwidth Usage in Real Time 58
Viewing the Top Users of Bandwidth 60
Viewing Bandwidth Usage Over Time 62
Viewing the Top Users of Bandwidth Over Time 63
Viewing Service Usage Reports 65
Monitoring Service Usage in Real Time 66
Viewing the Services Summary Report 67
Viewing Web Usage Reports 68
Viewing the Web Usage Summary Report 69
Viewing the Top Sites 70
Viewing the Top Users of HTTP Bandwidth 72
Viewing HTTP Bandwidth Usage by User 75
Viewing Bandwidth Usage Over Time 76
Viewing Top Sites Over Time 77
Viewing Top Users Over Time 79
Viewing Bandwidth Usage By User Over Time 82
Viewing Web Filter Reports 84
Viewing the Web Filter Summary Report 84
Viewing the Web Filter Top Sites Report 86
Viewing the Top Users that Try to Access Blocked Sites 88
Viewing the Top Blocked Sites for Each User 91
Viewing Blocked Site Attempts Over Time 93
Viewing the Top Blocked Site Attempts Over Time 94
Viewing the Top Blocked Site Users Over Time 96
Viewing the Top Blocked Sites for Each User Over Time 99

Viewing File Transfer Protocol Reports 101
Viewing the FTP Summary Report 101
Viewing the Top Users of FTP Bandwidth 103
Viewing FTP Bandwidth Usage Over Time 106
Viewing the Top Users of FTP Bandwidth Over Time 107
Viewing Mail Usage Reports 110
Viewing the Mail Usage Summary Report 110
Viewing the Top Users of Mail Bandwidth 112
Viewing Mail Usage Over Time 115
Viewing the Top Users of Mail Bandwidth Over Time 116
Viewing VPN Usage Reports 119
Viewing the VPN Usage Summary Report 119
Viewing the Top VPN Users 121
Viewing VPN Usage Over Time 124
Viewing the Top VPN Users Over Time 125
Viewing Attack Reports 128
Viewing the Attack Summary Report 128
Viewing the Attacks by Category 130
Viewing the Attacks by Source 132
Viewing the Errors and Exceptions Report 134
Viewing Attack Reports Over Time 136
Viewing Errors Over Time 138
Categories Over Time 140
Sources Over Time 142
Viewing Authentication Reports 144
Viewing the User Login Report 144
Viewing the Administrator Login Report 146
Viewing the Failed Login Report 147
Viewing the Log 149
Technical Tips 151
Viewing the ViewPoint Database Port Number 151
Changing the ViewPoint Web Server Port Number 151
Changing the ViewPoint Server IP Address 152
Changing the Default Syslog Server Port Number 152
The SonicWALL ViewPoint Log Files 152
Encrypting the sgmsConfig.xml File 153
Resetting the Admin Password 153
Copying and Pasting into the ViewPoint User Interface 153
Configuring Secure (HTTPS) Access 154
Creating a Secure Website 155

Securely Accessing SonicWALL ViewPoint **156**
Troubleshooting **159**
Installation Failure **159**
Viewpoint Cannot Install SQLAgent Service **160**
ViewPoint Cannot Connect to the MSDE Database **161**
ViewPoint Cannot Locate the MSDE Database **161**
ViewPoint Cannot Install Due to an Unexpected Signal Error ... **162**

About this Book

Welcome to the SonicWALL ViewPoint User's Guide. This guide provides the information you need to successfully install, configure, and administer the SonicWALL ViewPoint application.

This document provides detailed instructions on how to configure your main and remote SonicWALL firewall/VPN appliances to send syslog data to ViewPoint. Once the syslog data is received and stored in the ViewPoint database, you can log into ViewPoint and view firewall activity reports such as Top Users Bandwidth, Summary Bandwidth, and Dropped Packets, to understand and control overall Internet usage and network activity.

The document also provides information about generating and viewing default and customized report types. The document describes the different types of ViewPoint reports in detail, and indicates whether the report can be generated for an individual appliance or a group of appliances.

Audience

The audience for this manual is network administrators who are concerned with Internet activity, network threats, inappropriate Web use, employee productivity, and bandwidth utilization. ViewPoint gives network administrators a highly sophisticated, economical reporting tool that allows them to easily monitor network access and Internet usage, enhance security, assess risks, understand more about employee Internet use and productivity, and anticipate future bandwidth needs.

Related Publications

For additional information about ViewPoint, consult the following:

- *SonicWALL ViewPoint Data Sheet*

Document Organization

This document is organized as follows:

Chapter 1	"Introducing SonicWALL ViewPoint"
Chapter 2	"Installing SonicWALL ViewPoint"
Chapter 3	"Configuring ViewPoint"
Chapter 4	"Viewing Reports"
Appendix A	"Technical Tips"
Appendix B	"ViewPoint Reports"

Document Conventions

This guide uses a variety of formats to highlight specific types of information.

Special Message Conventions

Special message conventions refer to noteworthy information, and include a symbol for quick identification:

Note: *Identifies information of importance or special interest.*

Visual Conventions

Visual conventions refer to specific types of information, formatted in a particular manner:

courier	Identifies syntax statements, URLs, and path, file, drive, directory, database, or table names.
`<courier>`	Identifies variable names.
courier bold	Identifies text you must type to complete a procedure.
italics	Identifies document and chapter titles, special words used for the first time, and email addresses.
Initial Caps	Identifies window, menu, dialog, command, button, option, tab, keyboard, and product-specific names.
ALL CAPS	Identifies acronyms and abbreviations.

Text Conventions

Text conventions refer to one- or two-word instructions.

Select	Directs you to either highlight text, or position the mouse over a cell, menu option, radio button, checkbox, or similar item.
Click	Directs you to position the mouse cursor over an on-screen object, then press and quickly release the primary mouse button (typically the left button).
Double-click	Directs you to position the mouse cursor over an on-screen object, then quickly press and release the primary mouse button two times in rapid succession.
Secondary-click	Directs you to position the mouse cursor over an on-screen object, then press and quickly release the mouse button that is *not* your primary mouse button (typically the right button).
Drag	Directs you to position the mouse cursor over an on-screen object, then press and hold down the primary mouse button. While still pressing the primary mouse button, move the mouse cursor to the position where you want to move the selected object. Release the mouse button.
Press	Directs you to press and hold down a keyboard key.

Additional Help

For additional information or assistance, contact:

Phone	1.888.777.1476 (North America), +408.752.7819, (within California)
Internet	http://www.sonicwall.com/support/index.html

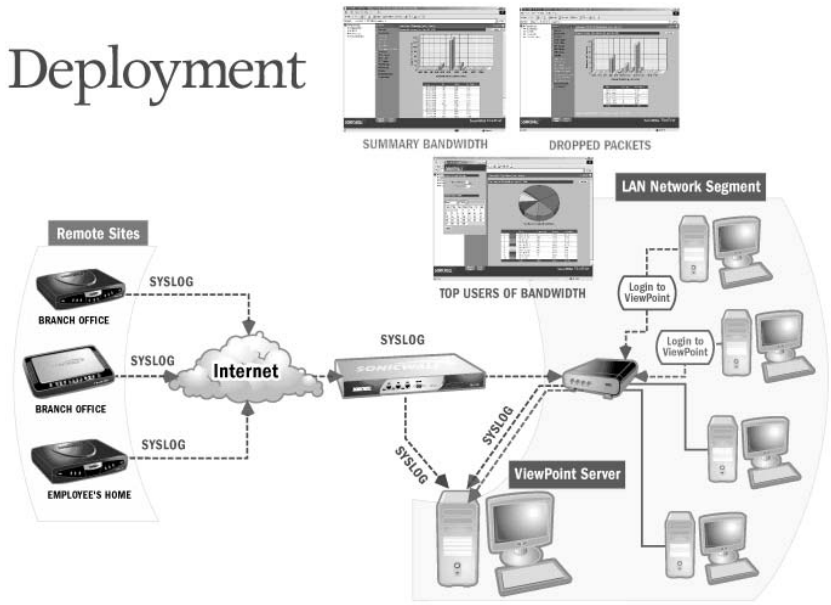
CHAPTER 1

Introducing SonicWALL ViewPoint

As a Web-based graphical reporting tool, ViewPoint provides unprecedented security awareness and control over your network environment through detailed and comprehensive reports of your network and firewall activities. ViewPoint's broad reporting capabilities allow administrators to easily monitor network access and Internet usage, enhance security, assess risks, understand more about employee Internet use and productivity, and anticipate future bandwidth needs.

ViewPoint creates dynamic, real-time and historical network summaries, providing a flexible, 360º view of network events and activities. Reports are based on "syslog" data streams received from each SonicWALL appliance through wired LAN, wireless LAN, WAN or VPN tunnel. With ViewPoint, your organization can generate individual or aggregate reports about virtually any aspect of appliance activity, including individual user or group usage patterns, events on specific appliances or groups of appliances, types and times of attacks, resource consumption and constraints, and more. An integral part of any deployment, ViewPoint delivers the comprehensive view of network and firewall activities your organization needs to enhance security and manage critical resources today and tomorrow.

Figure 1: ViewPoint Architecture



Key Features & Benefits

Ease-of-Use—ViewPoint features an easy-to-follow Installation Wizard to quickly install the product. ViewPoint includes an integrated Web server, syslog server, scheduling and summarization engines, and embedded database for fast, one-step installation.

Web-based User Interface—All reporting functions are performed from ViewPoint's intuitive Web User Interface, simplifying deployment and access from a local or remote system using a Web browser application. ViewPoint also allows multiple users to log into the application as the same admin user, allowing greater flexibility in administration.

Comprehensive Set of Graphical Reports—ViewPoint offers a comprehensive set of graphical reports including firewall attacks, bandwidth usage, Web site visits, user activity, and more, allowing organizations to be aware of suspicious activity and to ensure high employee productivity.

On-Demand Reporting—ViewPoint provides immediate reporting functionality for users requiring quick results, saving time and administration overhead.

Aggregate Reports—Supports multiple firewalls, allowing organizations with more than one firewall to view aggregate reports of their firewall activities from a single application to better understand their Internet bandwidth usage and plan for future capacity needs.

Reports of Custom Services - ViewPoint generates Summary and Monitor reports for custom-defined services, offering users insight into the activities of their specific applications.

Automated Report Scheduling - ViewPoint provides support for automatic e-mailing and archiving daily/weekly/monthly reports at scheduled intervals, allowing you to share the data with your colleagues and management team, and to store it for future use.

Flexible Number of Top Users and Sites - ViewPoint provides the flexibility to view reports for a large range of top sites, top users, and top sites per user, including 5, 10, 20, 50, and 100.

Reporting Based on User Accounts - ViewPoint provides support for reports based on individual user names instead of the IP address or hostname of their systems, revealing how the company employees are using the Internet.

Content Filtering Service (CFS) Category Reporting - ViewPoint creates categorized reports on the active users and the filtered web sites that they have attempted to visit. ViewPoint provides list of CFS categories, including CFS Premium categories, in all the Web Filter Top User and Top Site reports.

Bandwidth Report per Interface - ViewPoint provides reports on incoming versus outgoing traffic per firewall interface so that you can understand how your bandwidth is being used. You can now see the on-demand Bandwidth Summary usage through interfaces, selecting source and destination interfaces and for uni- and bi-directional traffic.

Log Viewer - ViewPoint provides users with the ability to search the database for a specific firewall activity type.

CHAPTER 2

Installing SonicWALL ViewPoint

This chapter describes how to install SonicWALL ViewPoint.

To install ViewPoint, complete the following procedures:

- Review the installation requirements. See “System Requirements” on page 20.
- Install ViewPoint, see “Installation” on page 20.
- Register ViewPoint, see “Registering ViewPoint” on page 25.

System Requirements

In order to install and run ViewPoint, you must be logged in as an administrator with full administrator access rights. The ViewPoint server must meet the following requirements:

- Windows 2000 Server, Windows 2000 Professional, Windows XP Professional, or Windows 2003.
- Pentium III or IV with a 1.4 GHz or faster processor.
- Minimum 512 MB RAM.
- At least 20 GB of free disk space.
- A hostname of 20 characters or less.
- The ViewPoint system must be connected to the network.
- ViewPoint cannot be installed in a folder that has an embedded blank space. For example, “Program Files.”
- ViewPoint requires a consistent destination IP address for communication with a SonicWALL. When communicating with a SonicWALL on the WAN management interface, the unit must have a static WAN IP address. If ViewPoint is communicating with a SonicWALL on the static LAN IP address, then the WAN interface can be dynamic or static.
- Local and remote browser access: Microsoft Internet Explorer 5.5 or later.
- Support for Java Plug-in JRE 1.4.1

Installation

Note: *If you are upgrading a previously installed version of ViewPoint, we strongly recommend that you back up your entire ViewPoint folder as well as the sgmsConfig.xml file, before proceeding with Phase 1 of the installation.*

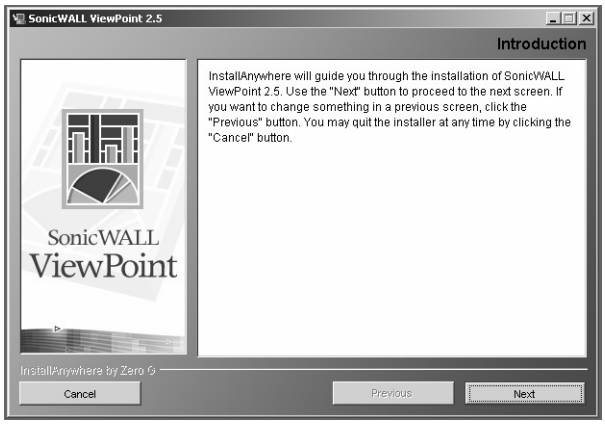
When you are ready to install ViewPoint, follow these steps:

1. Log on to the computer as administrator.

Note: *You must have full administrator access rights to install this application.*

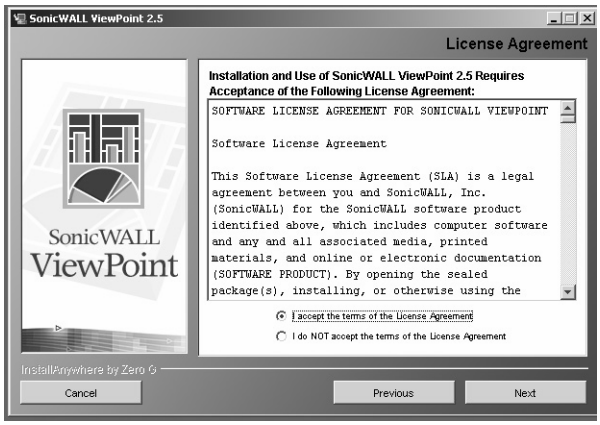
2. Locate the ViewPoint install file on the network. Double-click the VPS.exe. The Introduction screen opens.

Figure 2: Introduction Screen


SonicWALL ViewPoint 2.5
Introduction
InstallAnywhere will guide you through the installation of SonicWALL ViewPoint 2.5. Use the "Next" button to proceed to the next screen. If you want to change something in a previous screen, click the "Previous" button. You may quit the installer at any time by clicking the "Cancel" button.
SonicWALL
ViewPoint
InstallAnywhere by Zero G
Cancel
Previous
Next

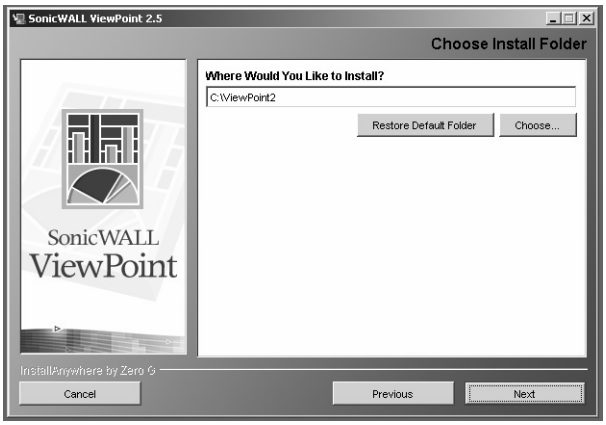
3. Click **Next**. The License Agreement screen opens.

Figure 3: License Agreement


SonicWALL ViewPoint 2.5
License Agreement
Installation and Use of SonicWALL ViewPoint 2.5 Requires Acceptance of the Following License Agreement:
SOFTWARE LICENSE AGREEMENT FOR SONICWALL VIEWPOINT
Software License Agreement
This Software License Agreement (SLA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package(s), installing, or otherwise using the
I accept the terms of the License Agreement
I do NOT accept the terms of the License Agreement
SonicWALL
ViewPoint
InstallAnywhere by Zero G
Cancel
Previous
Next

4. Select from the following:
   - To accept the terms of the license agreement, select **I accept the terms of the License Agreement** and click **Next**. The Choose Install Folder screen opens.
   - To not accept the terms, select **I do NOT accept the terms of the License Agreement** and click **Next**. The SonicWALL ViewPoint installation program closes and the product does not install,

Figure 4: Choose Install Folder

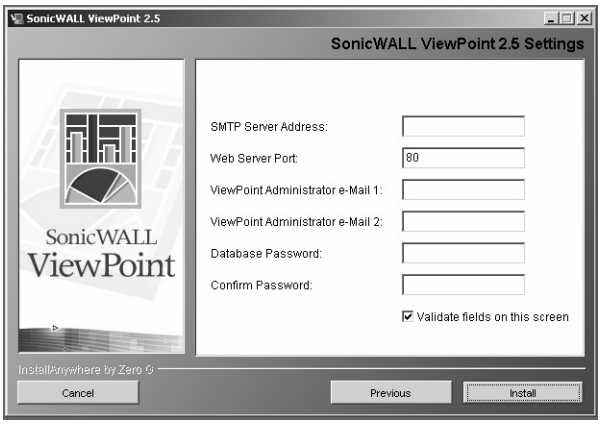


5. To accept the default location, click **Next**. To select a different location, click **Choose** and select a folder. Click **Next**.

   Note: *Figures 4 and 5 do not appear during an upgrade installation. The Upgrade screen appears.*

   The Settings screen opens.

Figure 5: Settings Screen



Do the following:

- Enter the IP address or host name of the Simple Mail Transfer Protocol (SMTP) server in the **SMTP Server Address** field.
- Enter the number of the web server port in the **Web Server Port** field (default: 80).
- Enter the e-mail addresses of administrators who will receive e-mail notifications from ViewPoint.

- Enter and confirm the database password in the **Database Password** and **Confirm Password** fields.
- To validate the entries on this page, select the **Validate fields on this screen** check box.

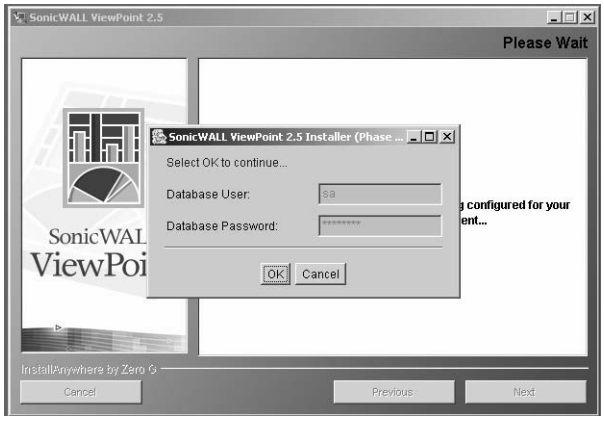
Click **Install**. The installation program begins copying ViewPoint files and installing the MSDE database.

Figure 6: Phase 2 Installer

SonicWALL ViewPoint 2.5
Phase 2 Installer Launch
To finish the installation, the installer will now launch the Phase 2 of the installer.
After installation of SonicWALL ViewPoint, to access the ViewPoint user interface (UI) from this system, you will be prompted to install the Java Plug-in 1.4.1_xx. Follow the plug-in installation instructions and once it is done, you will be able to access the ViewPoint UI. You will need to install this plug-in on any system from where you would like to access the ViewPoint UI.
When finished installing ViewPoint, you can access ViewPoint UI by double-clicking the "SonicWALL ViewPoint 2.5" shortcut on your desktop.
SonicWALL
ViewPoint
InstallAnywhere by Zero G
Cancel
Previous
Next

6. Click **Next**. Phase 2 of the installation begins.

Figure 7: Database Settings



7. Click **OK**.

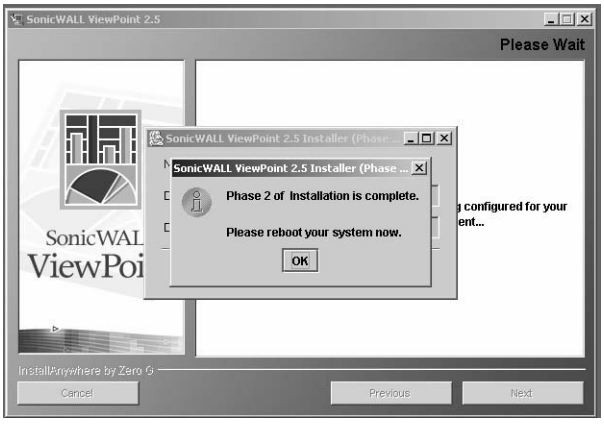
   Note: *The database name "sa" cannot be changed.*

Figure 8: Database Setup Progress Indicator

.

The installation program begins installing the database components. When it is finished, the Install Complete screen opens.

Figure 9: Installation Complete



8. Click **OK**. Installation is complete.
9. Restart the server.
10. Ensure the following ViewPoint services are running on your system:
    - SNWL ViewPoint Summarizer
    - SNWL ViewPoint Scheduler
    - SNWL ViewPoint Syslog
    - SNWL ViewPoint Web Server
    - MSSQL$SNWL (MSDE database)

Registering ViewPoint

To register ViewPoint, follow these steps:

- Create a mysonicwall.com account—see “Creating a mysonicwall.com Account” on page 25.
- Register the SonicWALL appliance—see “Registering a SonicWALL Appliance” on page 25.
- Activate the ViewPoint Software—see “Activating Your ViewPoint Software” on page 26.
- Enable the ViewPoint license on the SonicWALL appliance—see “Enabling the ViewPoint License” on page 27.

Creating a mysonicwall.com Account

If you do not already have a mysonicwall.com account, open a web browser and navigate to the following Web site:

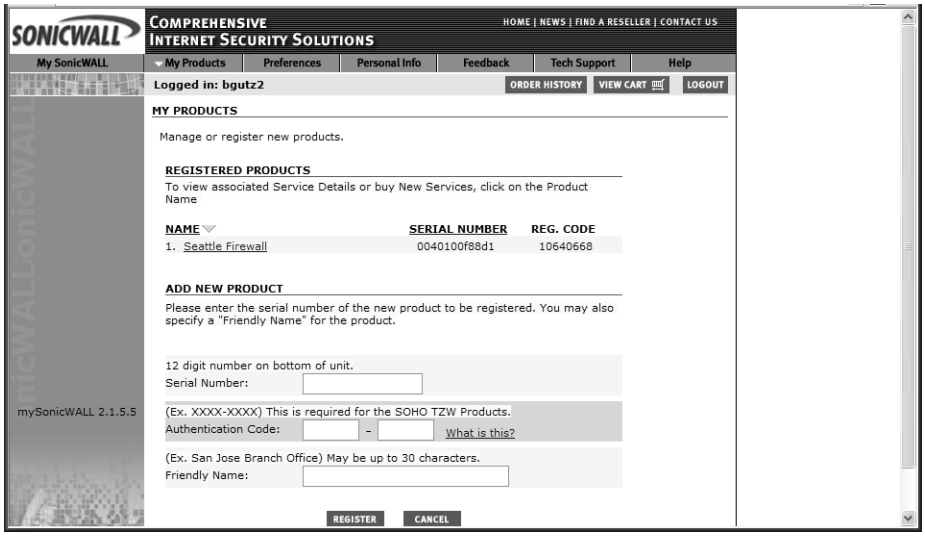
`http://www.mysonicwall.com`

Follow the on-screen prompts to create a user account.

Registering a SonicWALL Appliance

To register a SonicWALL appliance, follow these steps:

1. Log on to your mysonicwall.com account.
2. Click **My Products**. The **SonicWALL Product Registration** page opens.



3. Enter your SonicWALL Appliance serial number in the **Serial Number** field.

4. If you are registering a SonicWALL SOHO TZW, enter the authentication code in the **Authentication Code** field.
5. Enter a descriptive name for the SonicWALL appliance in the **Friendly Name** field.
6. Click **Register**. The mysonicwall.com website registers the SonicWALL appliance.

Activating Your ViewPoint Software

Note: *ViewPoint activation is not necessary for the following appliances:*

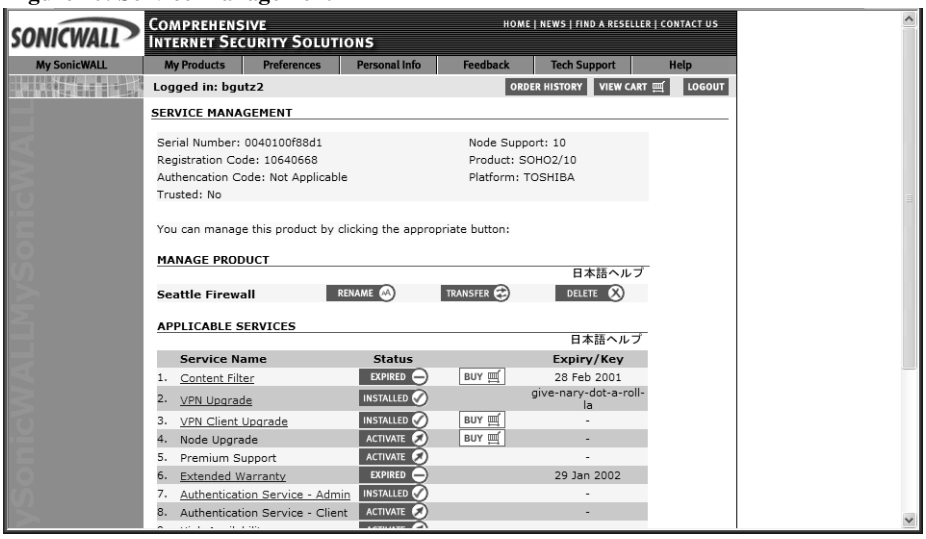
- *SonicWALL Pro 300*
- *SonicWALL Pro 330*
- *SonicWALL GX*

ViewPoint activation for these appliances occurs during registration. When the appliances are registered, ViewPoint is enabled by default. Use the procedure described below for all other SonicWALL appliances.

To activate your ViewPoint software, follow these steps:

1. Log on to your mysonicwall.com account.
2. Click the label of the newly registered SonicWALL appliance. The **Service Management** page opens.

Figure 10: Service Management



3. Locate the ViewPoint service and click its **Activate** button. The Activate Service dialog box opens.
4. Enter the ViewPoint Activation Key in the **Activation Key** field. The ViewPoint Activation Key is printed on the ViewPoint Software License Certificate shipped with the ViewPoint package.
5. Click **Submit**. After the Activation Key is registered, a ViewPoint License Key opens.

Note: *ViewPoint opens as an active licensed product under the SonicWALL appliance in your mysonicwall.com account.*

Enabling the ViewPoint License

To enable the ViewPoint license, follow these steps:

If the SonicWALL appliance is running **firmware 6.3.1.4 or greater**, follow these steps:

1. Log into the SonicWALL appliance.
2. Click **Log** and click **ViewPoint**. The **ViewPoint** page opens.
3. Enter the ViewPoint License Key provided by mysonicwall.com in the **Enter upgrade key** field.
4. Click **Upgrade**.
5. Restart the SonicWALL appliance for the change to take effect.

If the SonicWALL appliance is running **SonicOS 1.0 or greater**, follow these steps:

1. Log into the SonicWALL appliance.
2. Click **Log**, and then **ViewPoint**. The **ViewPoint** page opens.
3. Enter the ViewPoint License Key collected from mysonicwall.com into the **Enter upgrade key** field.
4. Click **Apply**.
5. Restart the SonicWALL appliance for the change to take effect.

   Note: *Activating your ViewPoint license can also be performed from the SonicWALL management interface using the Licenses page.*

CHAPTER 3

Configuring ViewPoint

This chapter explains how to configure SonicWALL ViewPoint. Select from the following:

- To begin the configuration process, see “Logging Into ViewPoint” on page 30.
- To configure a SonicWALL appliance for ViewPoint, see “Logging Into ViewPoint” on page 30.
- To configure access settings, see “Configuring Access to a SonicWALL Appliance” on page 33.
- To add a SonicWALL appliance to ViewPoint, see “Adding a SonicWALL Appliance to ViewPoint” on page 35.
- To delete a SonicWALL appliance from ViewPoint, see “Deleting a SonicWALL Appliance from ViewPoint” on page 38.
- To modify a SonicWALL appliance’s settings, see “Modifying Settings for a SonicWALL Appliance” on page 39.
- To change the ViewPoint password, see “Changing Your ViewPoint Login Password” on page 40.
- To configure ViewPoint settings, see “Configuring ViewPoint Settings” on page 41.
- To view and manage ViewPoint logs, see “Viewing and Managing ViewPoint Logs” on page 42.
- To manage ViewPoint sessions, see “Managing ViewPoint Sessions” on page 43.
- To configure reporting settings, see “Summarizer Settings” on page 46.

Logging Into ViewPoint

To start and log into ViewPoint:

1. If you are **logging in locally**, double-click the ViewPoint icon on your desktop.

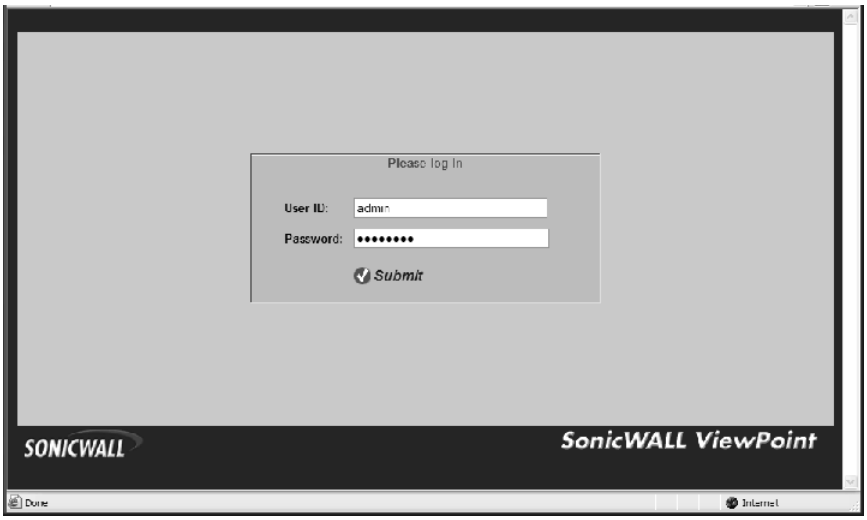
   If you are **logging in from a remote location**, open a web browser and enter

   http://*viewpoint_ipaddress*/sgms/login

   or

   http://*viewpoint_ipaddress*.

   where *viewpoint_ipaddress* is the IP address or hostname of the ViewPoint server.
2. The ViewPoint login page opens.



3. Enter the ViewPoint user ID (**admin)** and password (**password**).
4. When you enter the password, an authenticated management session begins. The session times out after 5 minutes of inactivity.
5. Click **Submit**. ViewPoint opens.
6. If you are prompted to install the Java Plug-in 1.4.1 application from Sun, click **Yes** and follow the on-screen instructions to install the Java Plug-in application.
7. To logout, click **Logout** in the ViewPoint user interface (UI).

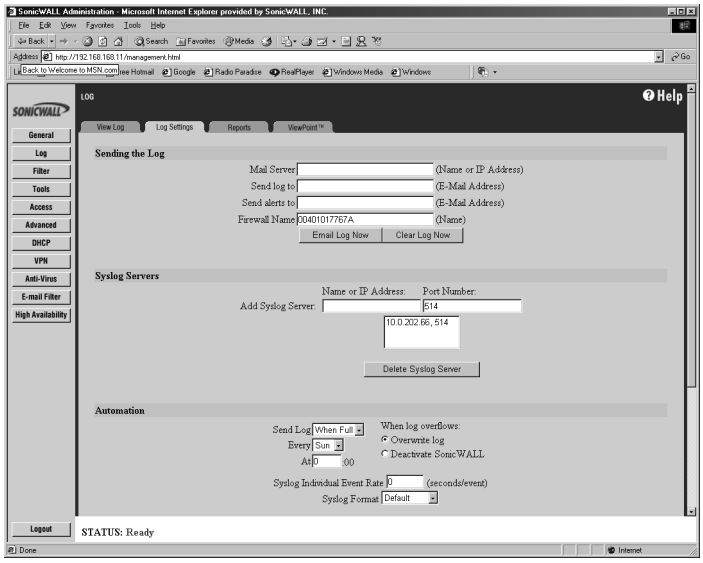
Note: *For security reasons, we recommend changing the default password for the admin user immediately after your first ViewPoint session begins. A password cannot exceed a length of 32 characters, and cannot contain special characters (e.g., # + , % &) nor embedded spaces.*

Configuring a SonicWALL Appliance for ViewPoint

The following instructions explain how to configure a SonicWALL appliance to send data to ViewPoint.

If the SonicWALL is running **firmware version 6.3.1.4,** or greater, follow these steps:

1. Log into the SonicWALL appliance.
2. Click **Log** and then click **Log Settings**. The **Log Setting**s page is displayed.



3. Enter the IP address or hostname and port number (default port number: 514) of the ViewPoint server in the **Add Syslog Server** fields.

   Note: *For firmware 6.3.1.4, the fields are* ***Syslog Server 1*** *and* ***Syslog Server Port 1****.*

4. Enter 0 in the **Syslog Individual Event Rate** field.

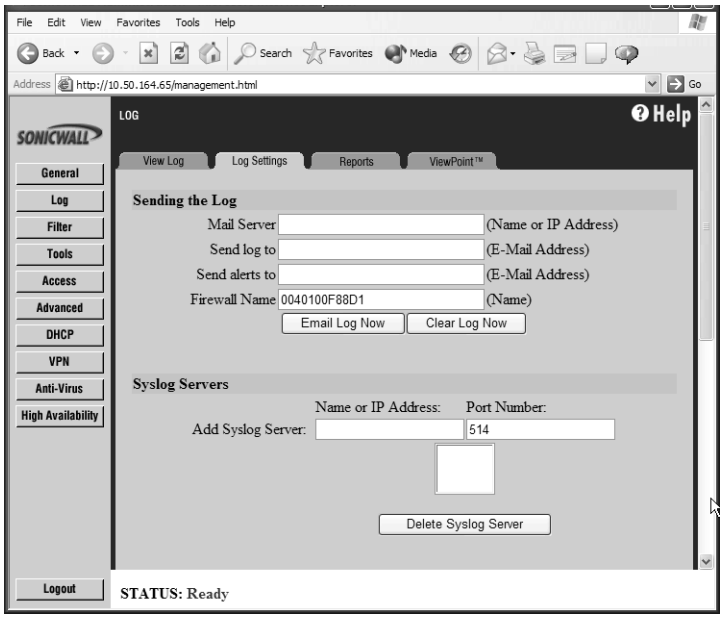
Note: *You can use the Syslog Individual Event Rate field to reduce the number of repetitive events logged by ViewPoint. Exercise caution when setting this value—entering a value greater than 0 excludes events from the log.*

5. Select **Default** from the **Syslog Format** list box.
6. To ensure accurate and complete reporting, make sure that every event category in the **Categories** area is selected except for **Network Debug**.
7. When you are finished, click **Update**.

Note: *ViewPoint expects the syslog data in UTC format. Make sure the* ***Display UTC in logs*** *check box on the General/Time screen for the SonicWALL appliance is selected.*

If the SonicWALL appliance is running **SonicOS version 1.0** or greater, follow these steps:

1. Log into the SonicWALL appliance.
2. Click **Log** and then click **Automation**. The Automation page opens.



3. Enter 0 in the **Syslog Individual Event Rate** field.

   Note: *You can use the Syslog Individual Event Rate field to reduce the number of repetitive events logged by ViewPoint. Exercise caution when setting this value—entering a value greater than 0 excludes events from the log.*

4. Select **Default** from **Syslog Format**.
5. Click **Add** in the **Server Name** section and enter the IP address or hostname and port (default: 514) of the ViewPoint server in the **Add Syslog Server** fields. Then, click **Apply**.
6. To ensure accurate and complete reporting, click **Categories** and make sure that every event category in the **Log Categories** area is selected except for **Network Debug**.
7. When you are finished, click **Apply**.

   Note: *ViewPoint expects the syslog data to come from a SonicWALL appliance in UTC format. Therefore, it is important that* ***Display UTC in logs*** *on the* ***System>Time*** *page in the SonicWALL appliance is selected.*

Configuring Access to a SonicWALL Appliance

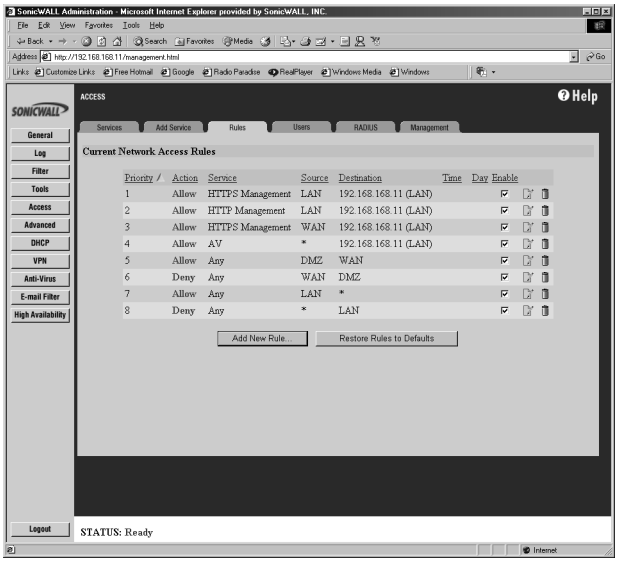
For reporting, your SonicWALL appliance must be added to the ViewPoint UI. To function properly, ViewPoint must be able to access, log into, and authenticate the ViewPoint license on the SonicWALL appliance. To accomplish this, ViewPoint can access the SonicWALL appliance from the LAN, WLAN, WAN, or over a VPN tunnel using HTTPS or HTTP.

- **LAN interface**—If the ViewPoint server is located on the same network as the SonicWALL appliance's LAN interface, ViewPoint can log into the SonicWALL appliance using HTTP or HTTPS. By default, both HTTP and HTTPS are enabled in your SonicWALL appliance. In this configuration, syslog traffic is sent to ViewPoint unencrypted.
- **VPN tunnel**—If the ViewPoint server is located behind a VPN/firewall device, and if there is a VPN tunnel between your SonicWALL appliance and the firewall, ViewPoint can access your SonicWALL appliance using HTTPS or HTTP over the VPN tunnel. In this configuration, syslog traffic is sent to ViewPoint encrypted.
- **WAN interface**—If the ViewPoint server is located on the WAN side of your SonicWALL appliance, the SonicWALL appliance can be configured to allow ViewPoint to access it using HTTPS. In this configuration, syslog traffic is sent to the ViewPoint server unencrypted.

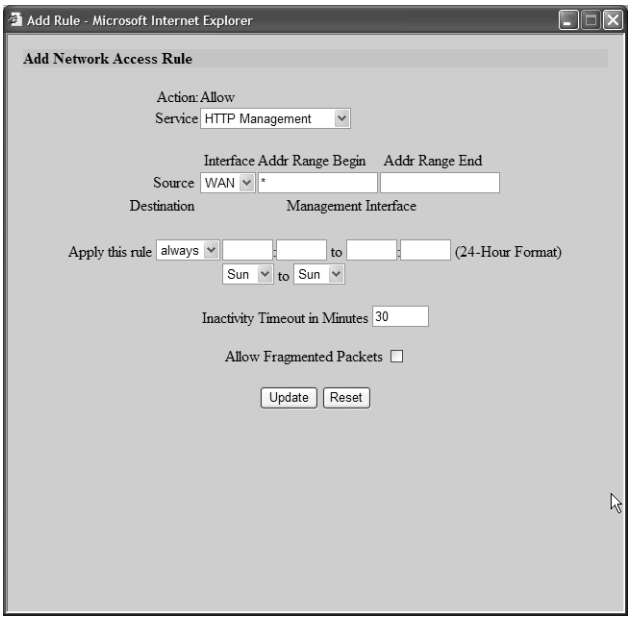
  Note: *If you use the WAN interface HTTPS option, the WAN IP address must be static. If the WAN IP address is dynamic, use the VPN tunnel option instead.*

  To enable WAN access using HTTPS:

1. Log into the SonicWALL appliance.
2. Expand the **Access** list, and click **Rules**. The Rules page opens.



3. Click **Add New Rule**. The **Add Network Access Rule** dialog box opens.


Add Rule - Microsoft Internet Explorer
Add Network Access Rule
Action: Allow
Service HTTP Management
Interface Addr Range Begin Addr Range End
Source WAN *
Destination Management Interface
Apply this rule always : to : (24-Hour Format)
Sun to Sun
Inactivity Timeout in Minutes 30
Allow Fragmented Packets
Update Reset

4. Create a rule that allows ViewPoint to access your SonicWALL appliance using HTTPS (HTTPS Management service) from the WAN and click **Update**. The rule is added.

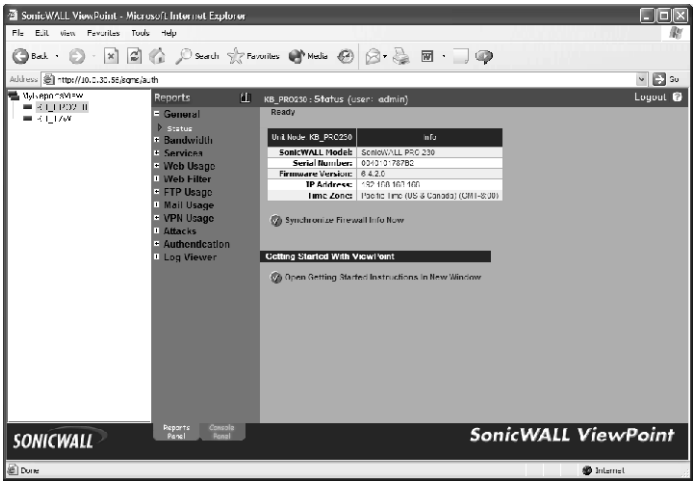
   Note: *The common name for the HTTPS Certificate must match the IP address or host name of the WAN interface.*

   Note: *If your ViewPoint server is behind a firewall, you need to ensure the syslog traffic can reach the ViewPoint server. To do this, add the IP address of the firewall as the syslog server in your SonicWALL appliance, and create a rule in the firewall to allow syslog traffic from your SonicWALL appliance to the ViewPoint server.*

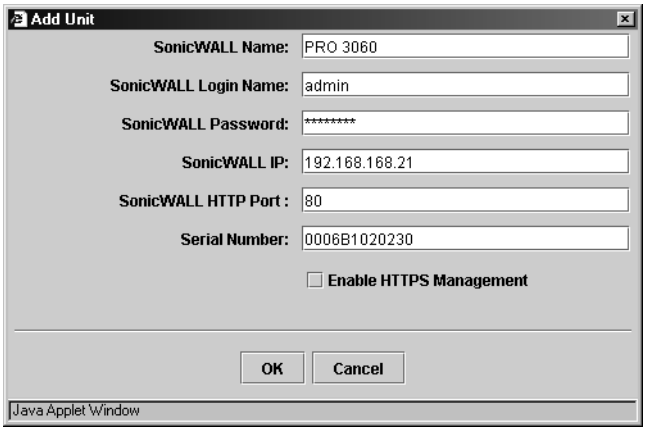
Adding a SonicWALL Appliance to ViewPoint

This section describes how to add a SonicWALL appliance to ViewPoint. To add a SonicWALL appliance, follow these steps:

1. Start and log into ViewPoint. The Status page opens.



2. Right-click MyReportsView in the left pane of ViewPoint and select **Add Unit** from the pop-up menu. The Add Unit dialog box opens.



3. Enter a descriptive name for your SonicWALL appliance in the **SonicWALL Name** field.

   Note: *Do not enter the single quote character (') in the SonicWALL Name field.*

4. Enter the username used to access your SonicWALL appliance in the **SonicWALL Login Name** field (default: admin).

   Note: *Do not enter a single quote (') in the* ***SonicWALL Login Name*** *field.*

5. Enter the password used to access the SonicWALL appliance in the **SonicWALL Password** field.

   Note: *Your ViewPoint password cannot exceed 32 characters, nor contain special characters (# + , % &) or embedded blank spaces.*

6. Enter the IP address used to access the SonicWALL appliance in the **SonicWALL IP Address** field.

   Note: *If ViewPoint is on the same LAN as the SonicWALL appliance or accesses it through a VPN tunnel, enter the LAN IP address. If ViewPoint accesses the SonicWALL appliance from the WAN interface, enter the static WAN IP address.*

7. If ViewPoint logs into the SonicWALL appliance using HTTP, deselect the **Enable HTTPS Management** check box and enter the HTTP port number used to access your SonicWALL appliance in the **SonicWALL HTTP Port** field (default: 80).

8. If ViewPoint logs into the SonicWALL appliance using secure HTTP (HTTPS), enter the HTTPS port number in the **SonicWALL HTTPS Port** field (default: 443).

9. Enter the serial number of the SonicWALL appliance in the **Serial Number** field.

   Note: *You must enter a valid value in all parameter fields in the Add Unit dialog box to continue this process.*

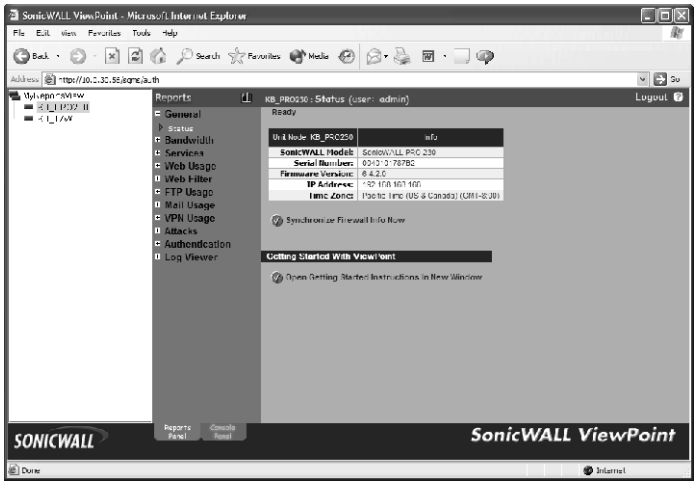
10. Click **OK**. ViewPoint finds the SonicWALL appliance and validates its ViewPoint license.

    Note: *When this procedure is complete, the SonicWALL appliance opens in the left pane of ViewPoint UI under My Reports View. If any of the parameters is entered incorrectly, an Authentication Failure message opens.*

Viewing and Updating SonicWALL Information

To view the status of a SonicWALL appliance, follow these steps:

1. Start and log into ViewPoint. The **Status** page opens.



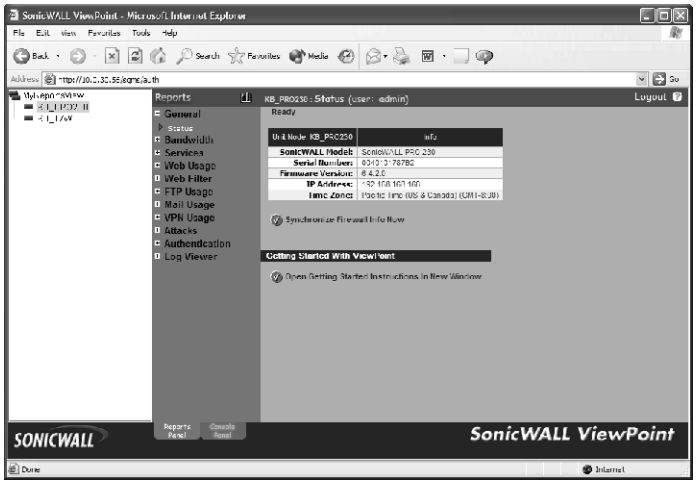
   The page displays the SonicWALL model, serial number, firmware version, IP address, time zone, ViewPoint licensing information, and the Syslog IP address configured on the SonicWALL.

2. This information is automatically updated every 24 hours. However, you can update the data at any time. To update this information, click **Synchronize Firewall Info Now**.

Deleting a SonicWALL Appliance from ViewPoint

To delete a SonicWALL appliance from ViewPoint, follow these steps:

1. Start and log into ViewPoint. The **Status** page opens.

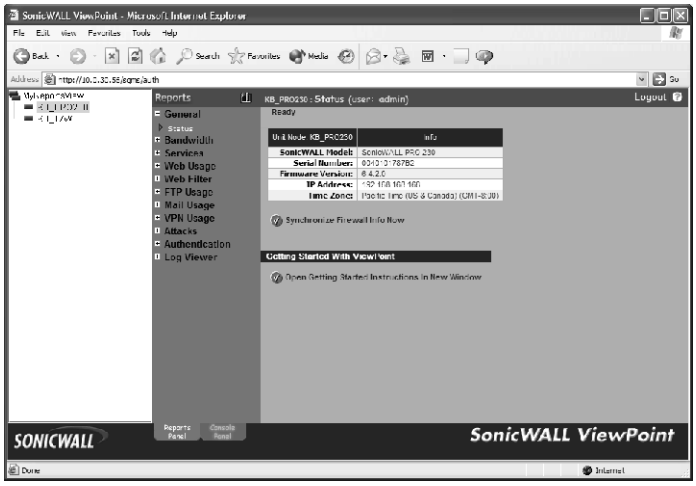


2. Select a unit under MyReportsView.
3. Right-click the unit and select **Delete** from the pop-up menu. You are prompted to confirm the deletion.
4. Click **Yes**. The SonicWALL appliance is removed from the left pane of the ViewPoint UI. The SonicWALL data is not deleted from the ViewPoint database.

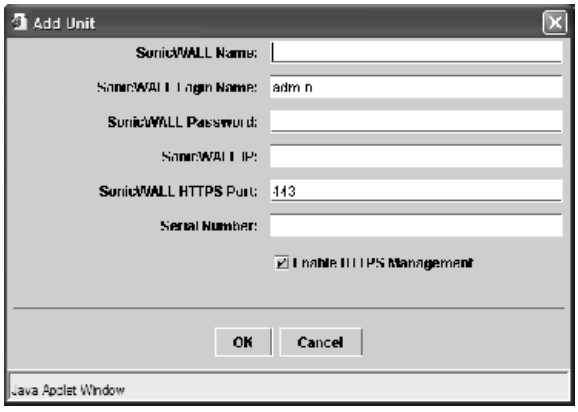
Modifying Settings for a SonicWALL Appliance

To change the settings of a SonicWALL appliance, whether you are changing the IP address, password, or other settings, follow these steps:

1. Start and log into ViewPoint. The **Status** page opens.



2. Select a unit in the left pane of the ViewPoint UI under MyReportsView.
3. Right-click on the unit and select **Modify Unit** from the pop-up menu. The Modify Unit dialog box opens.



4. Make changes to any of the fields.When you are finished, click **OK**. After ViewPoint finds the SonicWALL appliance and validates its ViewPoint license, the SonicWALL re-appears in the left pane under MyReportsView, and the ViewPoint database is modified.

Note: *Do not enter the single quote character (‘) in the SonicWALL Name field.*

Note: *Your ViewPoint password cannot exceed 32 characters, nor contain special characters (# + , % &) or embedded blank spaces.*

Note: *If the ViewPoint server is on the same network as the SonicWALL appliance LAN interface or if the ViewPoint server needs to access the SonicWALL appliance through a VPN tunnel, enter the LAN IP address of the SonicWALL appliance in the* ***IP Address*** *field. If the ViewPoint server accesses the SonicWALL appliance from the WAN, enter the WAN IP address of the SonicWALL appliance in the* ***IP Address*** *field. The WAN IP address must be static.*

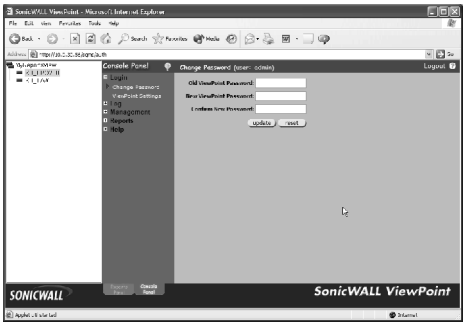
Note: *The serial number cannot be changed in the Modify Unit dialog box. To change this value, see the instructions “Modifying the Serial Number of an Appliance” on page 137.*

Changing Your ViewPoint Login Password

To modify the configuration settings for ViewPoint, follow these steps.

1. Start and log into ViewPoint.
2. Click the **Console Panel** tab at the bottom of ViewPoint .
3. Expand the **Settings** tree and click **User Settings**. The **User Settings** page opens.

Figure 11: User Settings



4. Enter the current ViewPoint password in the **Old ViewPoint Password** field.
5. Enter the new ViewPoint password in the **New ViewPoint Password** field.

6. Reenter the new ViewPoint password in the **Confirm ViewPoint Password** field.
7. **ViewPoint Inactivity Timeout** specifies how long ViewPoint waits before logging out an inactive user. To prevent someone from accessing ViewPoint while you are away from your desk, enter an appropriate value in the **ViewPoint Inactivity Timeout** field (the default is 5 minutes).

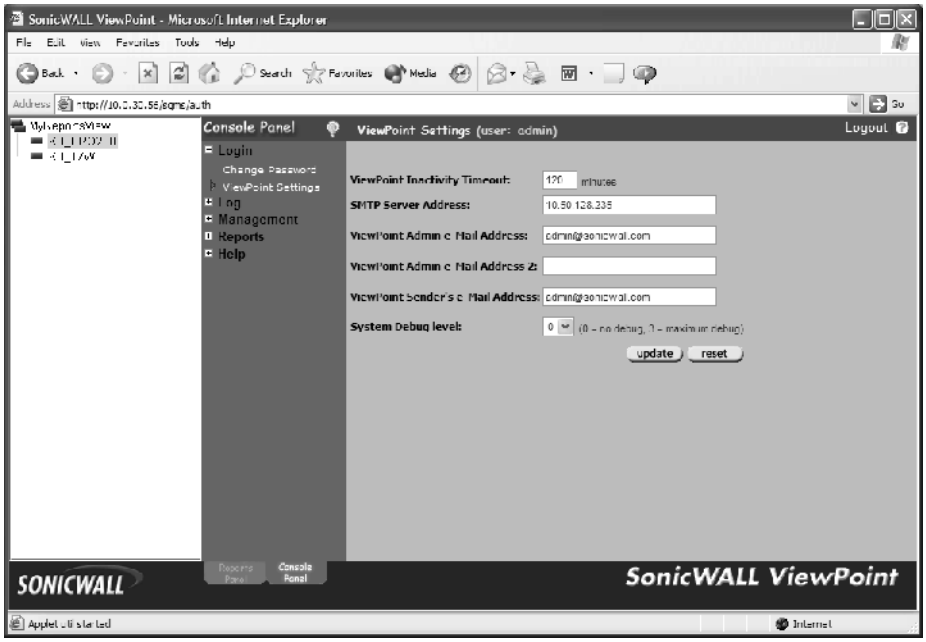
   Note: *This field can be set to a maximum of 32767 minutes.*
8. When you are finished, click **Update**. The password is changed. To clear all screen settings and start over, click **Reset**.

   Note: *The ViewPoint password cannot exceed 32 characters, nor contain special characters (# + , % &) or embedded blank spaces.*

Configuring ViewPoint Settings

To modify the configuration settings for ViewPoint, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Console Panel** tab at the bottom of the ViewPoint UI.
3. Expand the **Settings** button and click **ViewPoint Settings**. The ViewPoint Settings page opens.



4. Enter the IP address or hostname of the Simple Mail Transfer Protocol (SMTP) server in the **SMTP Server Address** field.
5. Enter the email addresses of the ViewPoint administrators in the **ViewPoint Admin e-Mail Address** and **ViewPoint Admin e-Mail Address 2** fields.

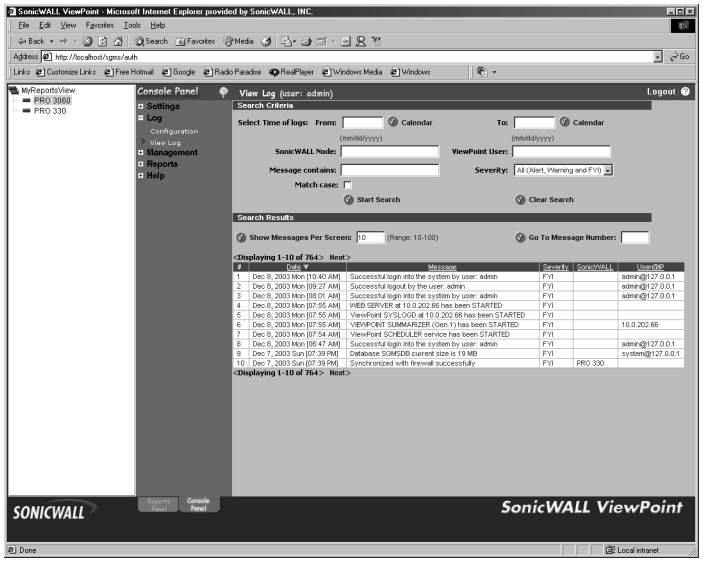
6. Enter the sender's email address that appears in messages sent from ViewPoint in the **ViewPoint Sender's e-Mail Address** field.
7. Select the amount of debug information that is stored from the **System Debug Level** field. For no debugging, enter 0. For verbose debugging, enter 3.

   Note: *Debugging should only be enabled when troubleshooting ViewPoint operational problems. See* *"Technical Tips and Troubleshooting" on page 151*.
8. When you are finished, click **Update**. The ViewPoint settings are changed. To clear the screen settings and start over, click **Reset**.

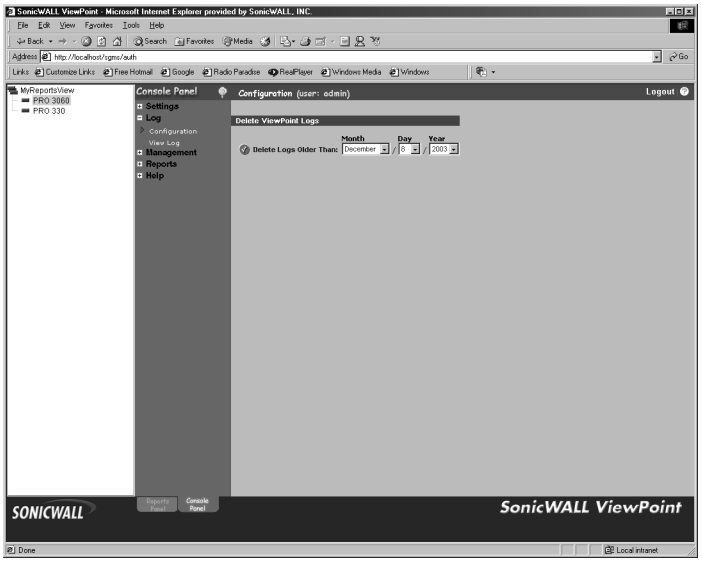
Viewing and Managing ViewPoint Logs

ViewPoint logs its activities. To view these logs, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Console Panel** tab at the bottom of the ViewPoint user interface.
3. Expand the **Log** tree and click **View Log**. The View Log page opens.



4. ViewPoint also allows you to delete the old logs. To do so, expand the **Log** tree and click **Configuration**. The Configuration page opens.



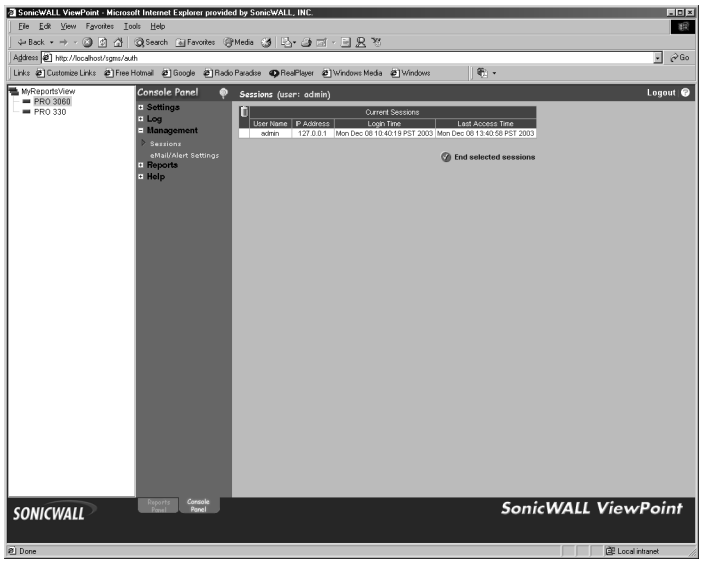
5. To delete logs older than a certain date, select the date and click **Delete Logs Older Than**.

Managing ViewPoint Sessions

To manage ViewPoint login sessions, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Console Panel** tab at the bottom of ViewPoint.

3. Expand the **Management** tree and click **Sessions**. The Sessions page opens.

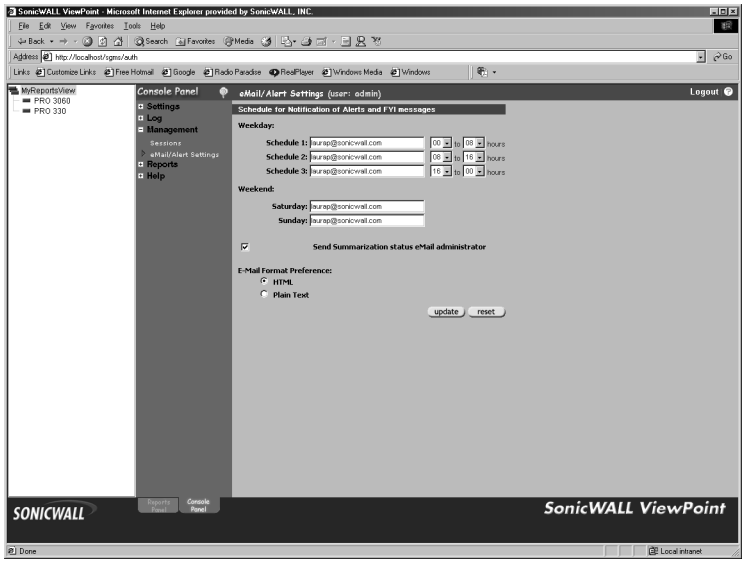


4. Select the check box of each user to log off and click **End selected sessions**. The selected users are logged off.

Configuring E-mail and Alert Settings

Alerts and FYI messages can be sent to your e-mail address during the week or on weekends. You can configure three e-mail addresses to received alerts and messages during the week and two e-mail addresses for weekend alerts and messages. In addition, the status of the data summarizer can be sent to you. To configure e-mail and alert settings, follow the steps below:

1. Start and log into ViewPoint.
2. Click the **Console Panel** tab at the bottom of ViewPoint.
3. Expand the **Management** tree, and click **eMail/Alert Settings**.



4. To schedule notification during the week, enter your e-mail address in the **Schedule 1** field. Select the time range from the **hours** menus. If this is the only e-mail address to receive alerts, select **00 to 00** as the hours range. If you have multiple e-mail addresses, enter these into the Schedule 2 and Schedule 3 fields. Select the time range from the **hours** menus.
5. To schedule notification during the weekend, enter your e-mail address in the **Saturday** and **Sunday** fields.
6. Leave **Send Summarization status eMail Administrator** checked to also send the status of the Summarization engine.
7. Select either HTML or Plain Text as your **E-Mail Format Preference**.
8. Click **Update**.

Summarizer Settings

This section describes how to configure reporting settings. These include how often the summary information is updated, the number of days summary information is stored, and the number of days raw data is stored.

ViewPoint reports are constructed from the **most currently available** summary data. In order to create summary data, ViewPoint must parse the raw data files.

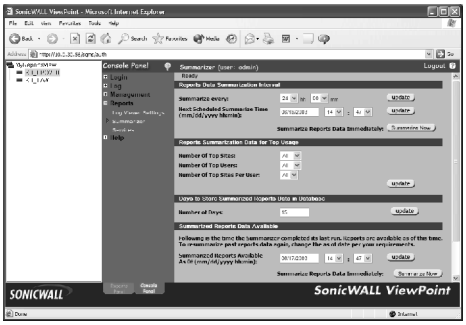
Note: *Typically, summarized data reaches a size of approximately 1Kb per SonicWALL appliance per day. Before specifying the number of days to store, consider the size of your database and, using the 1KB per appliance per day approximation, determine the number of days accordingly.*

Additionally, you can select the amount of raw data to store. The raw data is made up of information for every connection. Depending on the amount of traffic, the raw data can quickly consume an enormous amount of space in your database.

General Report Settings

To configure ViewPoint settings, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Console Panel** tab at the bottom of the ViewPoint user interface.
3. Expand the **Reports** tree and click **Summarizer**. The Summarizer page opens.



4. Specify how often ViewPoint processes and updates summary information from the **Summarize Every** list box. Click **Update**.
5. To specify the next summary time, enter a date and time in the **Next Scheduled Summary Time** field. Click **Update**.
6. To update the summary information now, click **Summarize Data Immediately**. ViewPoint automatically processes the latest information and makes it available for immediate viewing. This does not affect the normally scheduled summarization.
7. Configure the following default report settings and click **Update**.
   - Select the default number of sites to be summarized from the **Number of Top Sites** list box (default: All).
   - Select the default number of users to be summarized from the **Number of Top Users** list box (default: All).
   - Select the default number of sites per user to be summarized from the **Number of Top Sites Per User** list box (default: All).
8. Specify how many days of summarized data ViewPoint will store in the database from the **Days To Store Summarized Data** list box. Click **Submit**. To save all information, enter **All** (default: 15 days).
9. To delete the summarized data for a specific day from the database, you can enter the date in the **Delete Summarized Data For (mm/dd/yyyy)**: fields.

Note: *Summarized data can grow quickly and consume mass quantites of storage space. Exercise caution when selecting how much raw information to store.*

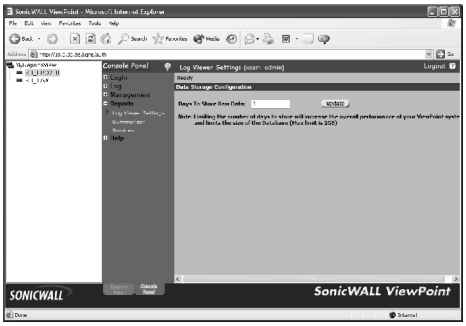
10. The **Summary Data Available Until** field displays when the data was last summarized. To re-summarize any data, enter a date and time and click **Update**.
11. If data is required for a date range, enter the date range in the **Summarize for a date range** fields using mm/dd/yyyy format.

Configuring Log Viewer Settings

To configure Log Viewer settings, follow these steps:

1. Start and log into ViewPoint.
2. Click the **Console Panel** tab at the bottom of the ViewPoint user interface.

3. Expand the **Reports** tree and click **Log Viewer Settings**. The Log Viewer Settings page opens.



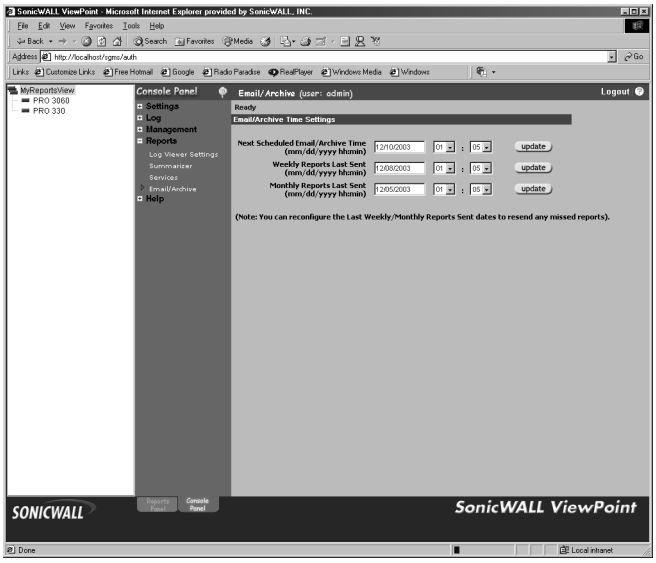
4. Specify how many days of raw data SonicWALL ViewPoint stores in the database from the **Days To Store Raw Data** field. Click **Update**. To save all information, enter **All** (default: 10 days).

Configuring Email/Archive Settings

To configure Email/Archive settings, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Console** tab.
3. Select a SonicWALL appliance.

4. Expand the Reports tree and click **Email/Archive**. The Email/Archive page appears.



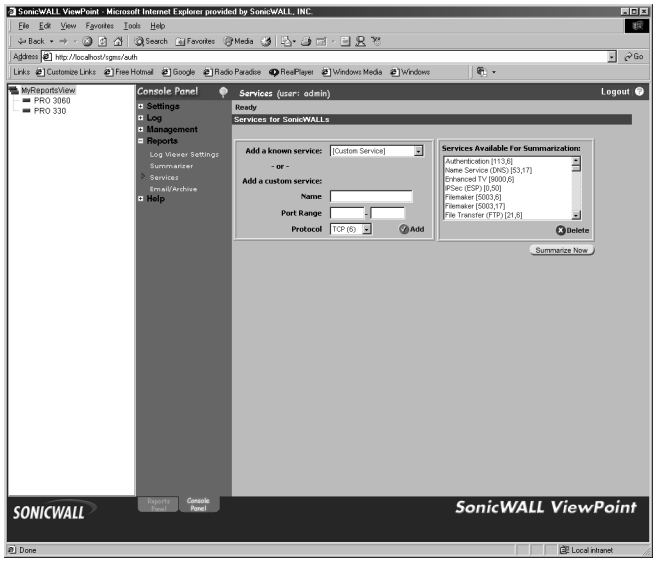
5. This page shows when the next scheduled archive time occurs and when the last weekly and monthly reports were sent.
6. To set the next archive time, enter the date and time in the **Next Scheduled Email/Archive Time** fields and click **Update**.
7. To specify when the next weekly report is sent, enter the date and time in the **Weekly Reports Last Sent** fields and click **Update**.
8. To specify when the next monthly report is sent, enter the date and time in the **Monthly Reports Last Sent** fields and click **Update**.

Adding a Service

ViewPoint can monitor known services or custom services.

To add a service that is displayed in the services reports, follow these steps.

1. Start and log into SonicWALL ViewPoint.
2. Click the **Console Panel** tab at the bottom of the ViewPoint user interface.
3. Expand the **Reports** tree and click **Services**. The Services page opens.



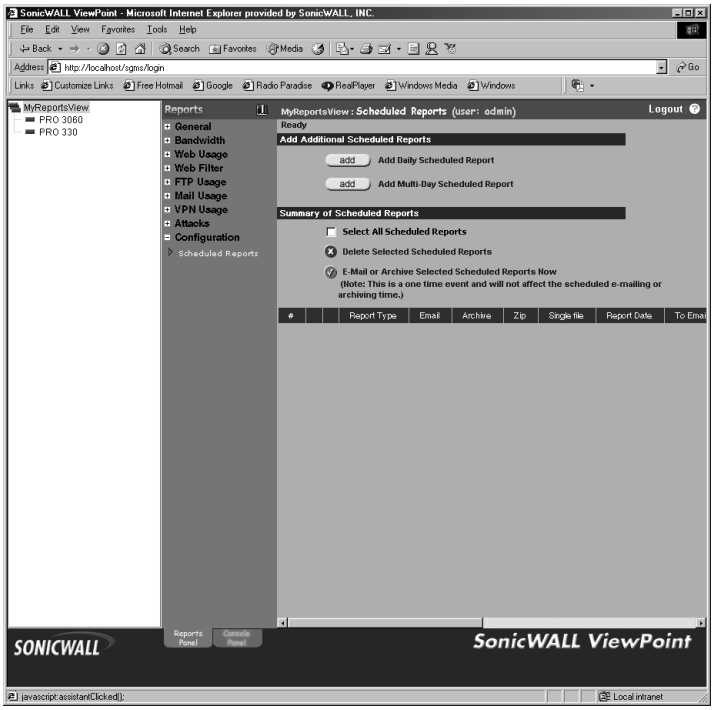
4. To add a known service, select it from the **Add a known service** list box. Click **Add**.
5. To add a custom service, enter a name in the **Name** field, enter the port range, and select the protocol used from the **Protocol** list box. Click **Add**.
6. To delete a service, select **from the Services Available for Summarization** menu and click **Delete**.

Scheduling ViewPoint Reporting

SonicWALL ViewPoint Reporting can automatically send reports to any specified e-mail addresses.

To view currently scheduled reports or configure new reports, follow these steps:

1. Start and log into ViewPoint.
2. Click **Reports Panel**.
3. Select a SonicWALL appliance.
4. Expand the **Configuration** tree and click **Scheduled Reports**. The Scheduled Reports page appears.



5. The Scheduled Reports page contains a list of currently scheduled reports. To edit a report, select its radio button and click **Edit**. To delete a report, select its radio button and click **Delete**.

   Note: *Scheduled reports are identified by their e-mail addresses. Therefore, modifying the e-mail address for a scheduled report creates another scheduled report.*

6. To e-mail a currently scheduled report now, click **E-mail Reports Now**.

   Note: *This does not affect the normally scheduled report.*
   Select from the following:

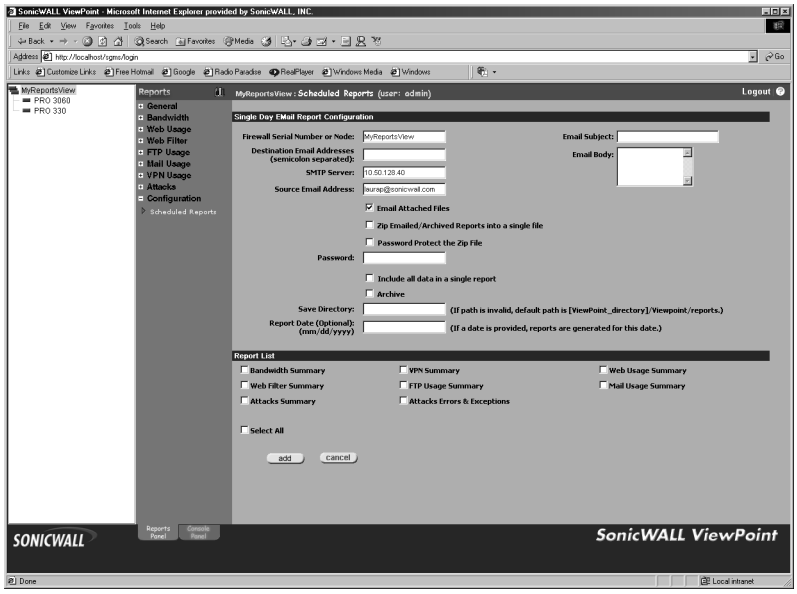
   - To create a new daily report, see “Scheduling a Daily Report” on page 52.
   - To create a new weekly or monthly report, see “Scheduling a Weekly or Monthly Report” on page 53.

Scheduling a Daily Report

Daily reports are sent out once a day at 03:00 GMT and contain information for the previous day. To configure a new daily report, follow these steps:

1. For all SonicWALL appliances, select **MyReportsView**.
1. From the Scheduled Reports page, click the **Add Daily Report** button. The Daily Reports page appears (Figure 12).

   Figure 12: Daily Reports Page



2. Enter the Destination e-mail addresses in the **Destination Email Addresses** field. Make sure each e-mail address is separated by a semicolon (;).
3. By default, ViewPoint uses the Simple Mail Transfer Protocol (SMTP) server that was specified during the SonicWALL ViewPoint installation. To change it, enter the IP address or hostname of the SMTP server in the **SMTP Server Address** field.
4. By default, ViewPoint uses the e-mail address of the user logged into ViewPoint as the Sender e-mail address. To change it, enter a new sender e-mail address in the **Source Email Address** field.
5. Enter the subject line to appear in reports sent from ViewPoint in the **Email Subject** field.
6. Enter text to appear in the message body in the **Email Body** field.
7. To send the file as an e-mail attachment, select the **Email Attached File** check box.
8. To compress the reports into a single file, select the **Zip Emailed/Archived Reports into a single file** check box.
9. To archive the file on the server's hard disk, select the **Archive** check box and enter a path in the **Save Directory** field.
10. **Optional.** To specify a specific date, enter the date in the **Report Date** field.
11. Select the daily reports to be included in the e-mail message:
12. Select the daily reports to be included in the e-mail message:

    - **Bandwidth Summary**—amount of traffic handled by the SonicWALL appliance during each hour.
    - **Web Filter Summary**—displays the number of times users attempt to access blocked sites during each hour.
    - **Attacks Summary**—number of attack attempted on the SonicWALL appliance.
    - **VPN Summary**— number of configured VPN tunnels and usage.

- **FTP Usage Summary**—amount of FTP bandwidth handled by the SonicWALL appliance.
- **Attacks Errors & Exceptions**—number of attempted attacks, system errors, and system exceptions.
- **Web Usage Summary**—amount of HTTP bandwidth handled by the SonicWALL appliance during each hour of the day.
- **Mail Usage Summary**—amount of mail handled by the SonicWALL appliance.

13. To add all of the reports to the schedule, use the **Select All** checkbox.
14. When you are finished, click **Add**. The new report appears in the list on the Scheduled Reports page.

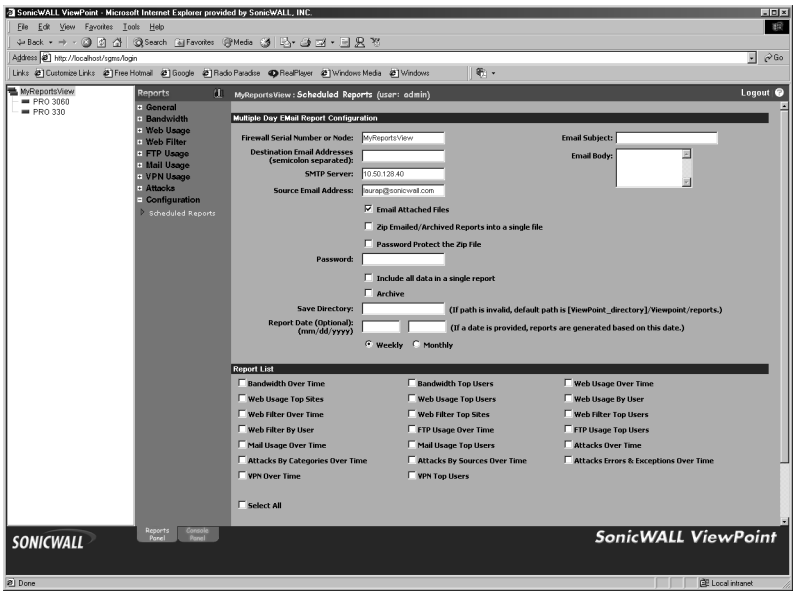
    Note: *If a single SonicWALL is selected, the* ***Report List*** *is the same as the Report List for weekly or monthly reporting. More categories are available to be included in the report.*

Scheduling a Weekly or Monthly Report

Weekly reports are sent out every Sunday at 03:00 GMT and contain information for the previous week. Monthly reports are sent out on the first day of every month at 03:00 GMT and contain information for the previous month. To configure a new weekly or monthly report, follow these steps:

1. From the Scheduled Reports page, click the **Add Multi-Day Report** button. The Multi-Day Reports page appears (Figure 13).

   Figure 13: Multi-Day Reports Page



2. Enter the Destination e-mail addresses in the **Destination Email Addresses** field. Separate each e-mail address with a semicolon (;).
3. Enter the IP address or hostname of the Simple Mail Transfer Protocol (SMTP) server in the **SMTP Server Address** field.
4. Enter the Sender e-mail address to appear in messages sent from ViewPoint in the **Source Email Address** field.
5. Enter the Subject Line to appear in reports sent from ViewPoint in the **Email Subject** field.
6. Enter text to appear in the message body in the **Email Body** field.
7. To send the file as an e-mail attachment, select the **Email Attached File** check box.
8. To compress reports into a single file, select the **Zip Emailed/Archived Reports into a single file** check box.
9. To archive the file to hard disk, select the **Archive** check box and enter a path in the **Save Directory** field.
10. **Optional.** To specify a specific date, enter the date in the **Report Date** field.
11. Select whether the report is sent **Weekly** or **Monthly**.
12. Select the reports to be included in the e-mail message:

- **Bandwidth Over Time**—displays the daily amount of traffic handled by a SonicWALL for the week or month.
- **Web Usage Top Sites**—displays the top Web sites accessed by users.
- **Web Filter Over Time**—displays the number of attempts that were made to access blocked Web sites for the week or month.
- **Web Filter By User**—displays accessing blocked Web sites by an individual user for the week or month.
- **Mail Usage Over Time**—displays the daily amount of mail handled by a SonicWALL for the week or month.
- **Attacks by Categories Over Time**—displays the number of attacks by category for the week or month.
- **VPN Overtime**—displays daily number of VPN connections during the week or month.
- **Bandwidth Top Users**—displays the top users of network bandwidth for the week or month.
- **Web Usage Top Users**—displays the top users accessing Web sites.
- **Web Filter Top Sites** — displays the top number of blocked Web sites.
- **FTP Usage Over Time**—displays the daily amount of FTP bandwidth handled by a SonicWALL for the week or month.
- **Mail Usage Over Time**—displays the amount of mail traffic for the week or month.
- **Attacks by Sources Over Time**— displays network attacks by the source for the week or month.
- **VPN Top Users**— displays the top users of VPN resources on the network for the week or month.
- **Web Usage Over Time**—displays the daily amount of HTTP bandwidth handled by a SonicWALL for the week or month.
- **Web Usage By User**—displays the top users accessing Web sites for the week or month.
- **Web Filter Top Users**—displays the top users attempting to access blocked Web sites for the week or month.
- **FTP Top Users**—displays the top users of FTP resources for the week or month.
- **Attacks Overtime**—displays the number of attacks attempted during the week or month.
- **Attacks Errors & Exceptions Over Time**— the number of attempted attacks, system errors, and system exceptions for the week or month.

13. To add all of the reports to the schedule, use the **Select All** checkbox.

CHAPTER 5

Viewing Reports

This chapter describes how to generate reports using SonicWALL ViewPoint.

Select from the following reports:

- To view general bandwidth usage reports, see “Viewing Bandwidth Reports” on page 55.
- To view bandwidth reports, by service, see “Viewing Service Usage Reports” on page 65.
- To view web usage bandwidth reports, see “Viewing Web Usage Reports” on page 68.
- To view reports on the number of attempts that users made to access blocked websites, see “Viewing Web Filter Reports” on page 84.
- To view file transfer protocol (FTP) bandwidth usage reports, see “Viewing File Transfer Protocol Reports” on page 101.
- To view mail bandwidth usage reports, see “Viewing Mail Usage Reports” on page 110.
- To view virtual private networking (VPN) reports, see “Viewing VPN Usage Reports” on page 119.
- To view reports on attempted attacks, see “Viewing Attack Reports” on page 128.
- To view detailed logging information, see “Viewing the Log” on page 149.
- To view user and administrator authentication reports, see “Viewing Authentication Reports” on page 144.

Note: *When you log into SonicWALL ViewPoint, ViewPoint displays data for the previous day. This is true for every new login session.*

Viewing Bandwidth Reports

Bandwidth reports display the amount of data transferred through the selected SonicWALL appliance(s).

Bandwidth reports are an ideal starting point for viewing overall bandwidth usage. You can view bandwidth usage view by the hour, day, or over a period of days. Additionally, you can view the top users of bandwidth.

From this information, you can determine network strategies. For example, if you need more bandwidth, you might need to upgrade network equipment, or you might simply need to curtail the bandwidth usage of a few employees.The following table lists the types of Bandwidth reports, and whether a report is available at the Unit or Group level.

Report Name	Unit Level	Group Level
Bandwidth Summary	Yes	Yes
Bandwidth Monitor	Yes	
Top Users of Bandwidth	Yes	
Bandwidth Usage Over Time	Yes	Yes
Top Users of Bandwidth Over Time	Yes	

Note: *The single firewall report opens in firewall's local time. The aggregate multi-firewall report opens in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view a summary of the daily bandwidth usage, see "Viewing the Bandwidth Summary Report" on page 56.
- To view bandwidth usage in real time, see "Monitoring Bandwidth Usage in Real Time" on page 58.
- To view the users who consume the most bandwidth, see "Viewing the Top Users of Bandwidth" on page 60.
- To view bandwidth usage over a period of time, see "Viewing Bandwidth Usage Over Time" on page 62.
- To view the users who consume the most bandwidth over time, see "Viewing the Top Users of Bandwidth Over Time" on page 63.

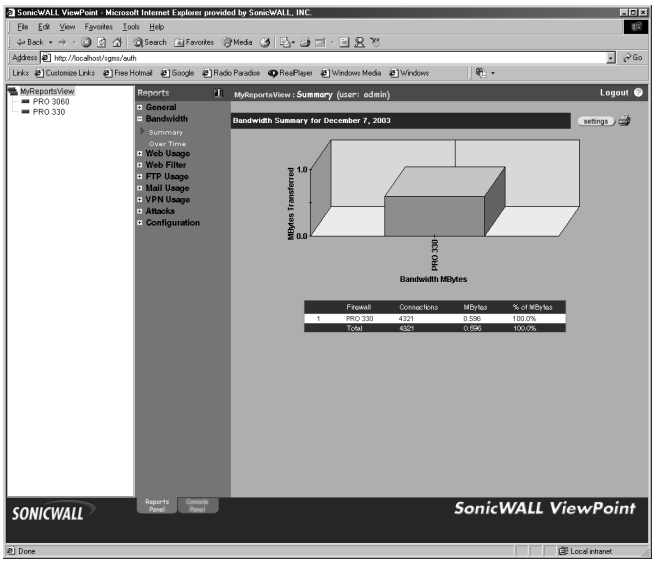
Viewing the Bandwidth Summary Report

The Bandwidth Summary report contains information on the amount of traffic handled by a SonicWALL appliance or group of SonicWALL appliances during each hour of the specified day.

To view the Bandwidth Summary report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the Bandwidth tree and click **Summary**. The Summary page opens.



5. The bar graph displays the amount of bandwidth transferred during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of events or "hits."
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field displays 10%.
7. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

   Note: *If ViewPoint is enabled on a SonicWALL running SonicOS Enhanced, bandwidth is also reported per interface.*

8. Select the year, month, and day to view.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

9. When you are finished, click **Close**. SonicWALL ViewPoint displays the report for the selected day.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

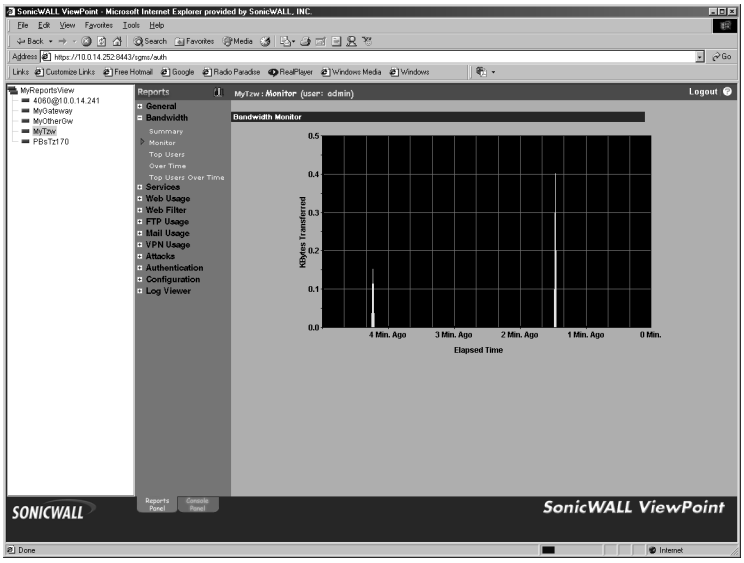
Monitoring Bandwidth Usage in Real Time

The Bandwidth Monitor displays bandwidth usage for the selected SonicWALL appliance in real time.

To view the Bandwidth Monitor, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Bandwidth tree and click **Monitor**. The Monitor page opens.



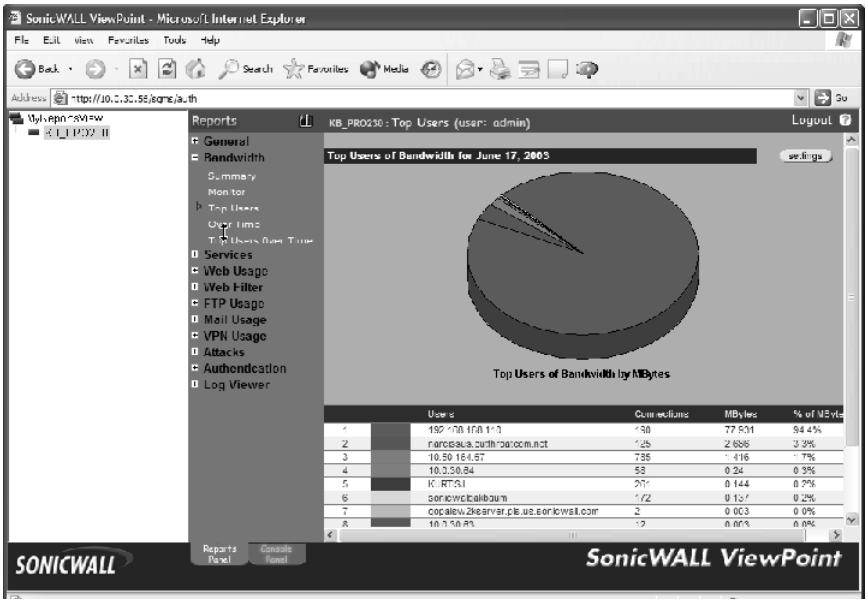
5. The Bandwidth Monitor shows the amount of data transferred during each sampling period for the last five minutes. The sampling period is five seconds.

Viewing the Top Users of Bandwidth

The Top Users report displays the users who used the most bandwidth on the specified date.

To view the Top Users report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Bandwidth tree and click **Top Users**. The Top Users page opens.



5. The pie chart displays the percentage of bandwidth transferred by each user.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of events or "hits."
   - **MBytes**—number of megabytes.
   - **% of MBytes—**percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the day and 200 megabytes was transferred by the top user, the **% of MBytes** field displays 20%.

7. By default, SonicWALL ViewPoint shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The ViewPoint Settings dialog box opens.

8. Select the number of users to display from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day to view.
11. If data is generated on a specific user, enter the name in the **Select Users** field. Use commas to separate the names.
12. When you are finished, click **Close**. SonicWALL ViewPoint displays the report for the selected day.

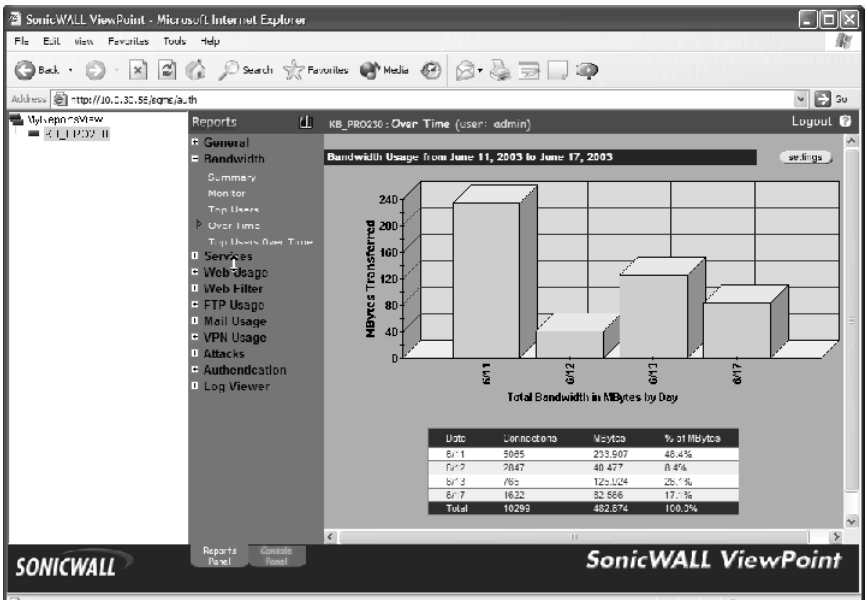
    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing Bandwidth Usage Over Time

The Bandwidth Over Time report displays the daily amount of traffic handled by a SonicWALL appliance or a group of SonicWALL appliances for the specified time period.

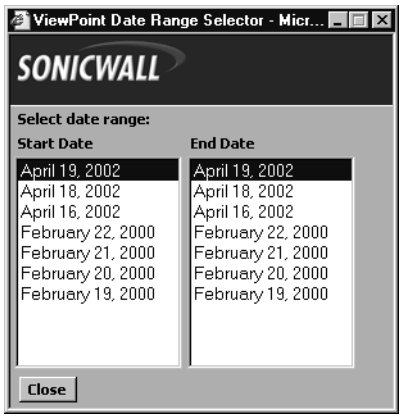
To view the Bandwidth Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Bandwidth tree and click **Over Time**. The Over Time page opens.



5. The bar graph displays the amount of bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **% of Usage**—percentage of megabytes transferred during this day, compared to the time period. For example, if 100,000 megabytes of data was transferred during the time period and 25,000 megabytes was transferred on one day, the **% of Usage** field displays 25%.
7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.

8. Select the starting and ending dates to view.



9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings will be reset to the default values embedded in the software.*

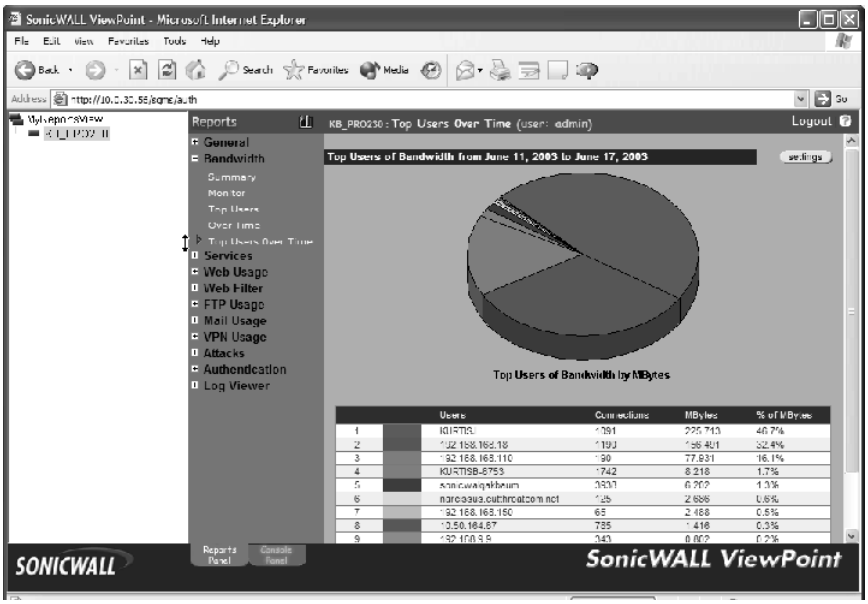
Viewing the Top Users of Bandwidth Over Time

The Top Users report displays the users who used the most bandwidth on the specified date.

To view the Top Users Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Bandwidth tree and click **Top Users Over Time**. The Top Users Over Time page opens.

5. The pie chart displays the percentage of bandwidth transferred by each user.



6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of events or "hits."
   - **MBytes**—number of megabytes.
   - **% of MBytes—**percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during this period and 200 megabytes was transferred by the top user, the **% of MBytes** field displays 20%.

7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.

8. Select the starting and ending dates to view.
9. If data is generated on a specific user, enter the name in the **Select Users** field. Use commas to separate the names.
10. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing Service Usage Reports

Service reports provide information on the amount of data transmitted through the selected SonicWALL appliance by each service.

Service reports are useful for revealing inappropriate usage of bandwidth and can help determine network policies. For example, if there is a large spike of bandwidth usage, you can determine whether this is caused by regular web access, someone using FTP to transfer large files, an attempted Denial of Service (DoS) attack, or another service.

Note: *The single SonicWALL report opens in SonicWALL's local time. You cannot view services reports for a group of SonicWALL appliances.*

SonicWALL ViewPoint can monitor known services as well as custom services. To add a service to monitor, refer to the documentation that accompanied the SonicWALL appliance.

Select from the following:

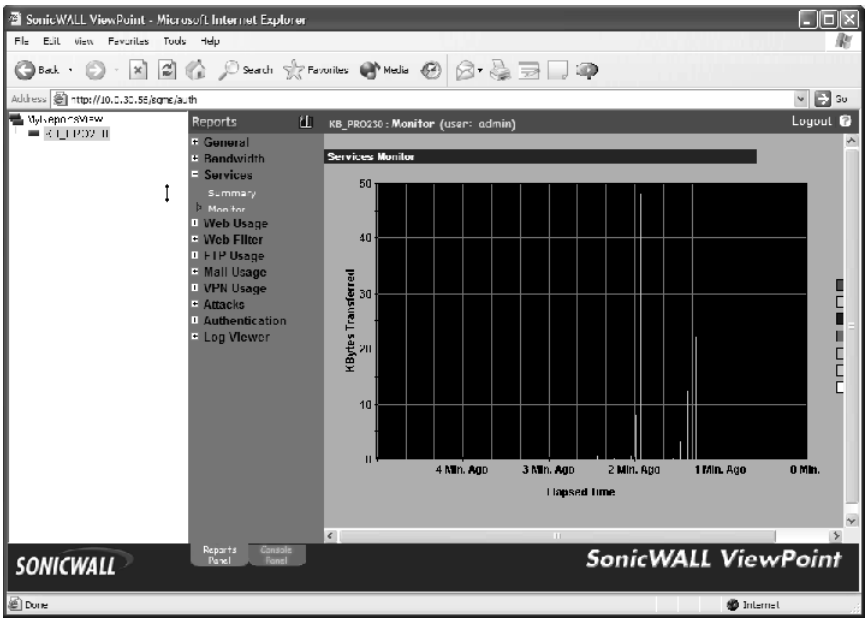
- To view service bandwidth usage in real time, see “Monitoring Service Usage in Real Time” on page 66.
- To view a summary of the daily service bandwidth usage, see “Viewing the Services Summary Report” on page 67.

Monitoring Service Usage in Real Time

The Services Monitor displays service usage for the selected SonicWALL appliance in real time.

To view the Service Monitor, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Services tree and click **Monitor**. The Monitor page opens.



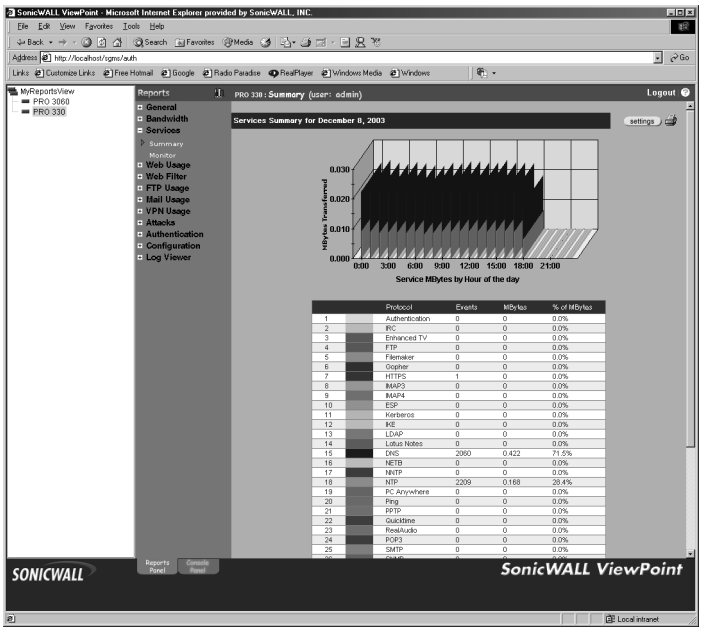
5. The Services Monitor shows the amount of data transferred for each service during each sampling period for the last five minutes. The sampling period is 15 seconds.

Viewing the Services Summary Report

The Services Summary report displays the amount of traffic handled by each service during each hour of the specified day.

To view the Services Summary report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Services tree and click **Summary**. The Summary page opens.



5. The bar graph displays the amount of bandwidth used by each service during each hour of the day.
6. The table contains the following information:
   - **Protocol**—the service.
   - **Events**—number of events or "hits."
   - **MBytes**—number of megabytes.
   - **% of MBytes**—percentage of MBytes transferred by this service on the selected day, compared to all other services. For example, if 100 MBytes were transferred during the day and 90 of the MBytes were handled by the HTTP service, the % of Events field displays 90%.

7. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

8. Select the year, month, and day to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings resets to the default values embedded in the software.*

Viewing Web Usage Reports

Web usage reports provide information on the amount of web usage that occurs through the selected SonicWALL appliance(s).

Web usage reports can be used to view web bandwidth usage by the hour, day, or over a period of days. Additionally, you can view the top users of web bandwidth and view the most visited sites.

The following table lists the type of Web Usage reports, and whether a report is available at the Unit or Group level.

Report Name	Unit Level	Group Level
Web Usage Summary	Yes	Yes
Top Visited Web Sites	Yes	
Top Users of Web	Yes	
Top Visited Web Sites by User	Yes	
Web Activity Over Time	Yes	Yes
Top Web Sites Over Time	Yes	
Top Web Users Over Time	Yes	
Top Sites By User Over Time	Yes	

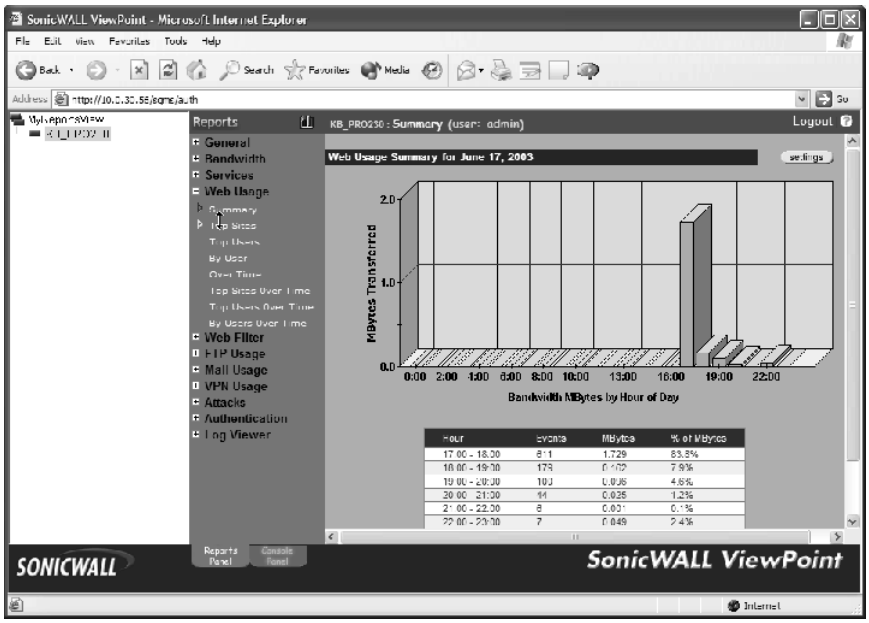
Note: *The single firewall report opens in the firewall's local time. The aggregate multi-firewall report opens in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Viewing the Web Usage Summary Report

The Web Usage Summary report contains information on the amount of HTTP bandwidth handled by a SonicWALL appliance or group of SonicWALL appliances during each hour of the specified day.

To view the Web Usage Summary report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Web Usage tree and click **Summary**. The Summary page opens.



5. The bar graph displays the amount of HTTP bandwidth transferred during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of events or "hits."
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of HTTP data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field displays 10%.

7. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

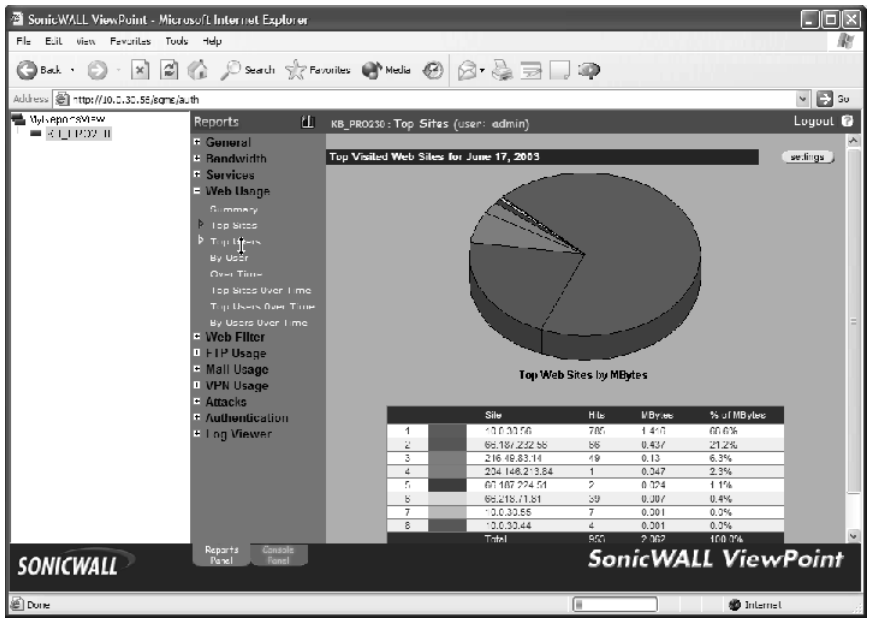
8. Select the year, month, and day to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

Viewing the Top Sites

The Top Sites report displays the web sites that used the most HTTP bandwidth on the specified date. To view the Top Sites report, follow these steps:

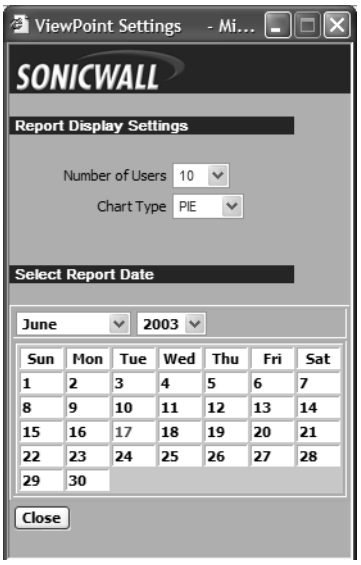
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Web Usage tree and click **Top Sites**. The Top Sites page opens.



5. The pie chart displays the percentage of bandwidth used to access the top sites.
6. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Hits**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred between this site, compared to all other HTTP traffic. For example, if 10,000 megabytes of data was transferred during the day and 5,000 megabytes was transferred between the appliance and Ebay, the **% of MBytes** field displays 50%.

7. By default, ViewPoint displays today's report, a pie chart, and the ten top sites. To change these settings, click **Settings**. The ViewPoint Settings dialog box opens.


ViewPoint Settings - Mi...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
June 2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

8. Select the number of sites to display from the **Number of Sites** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day to view.
11. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

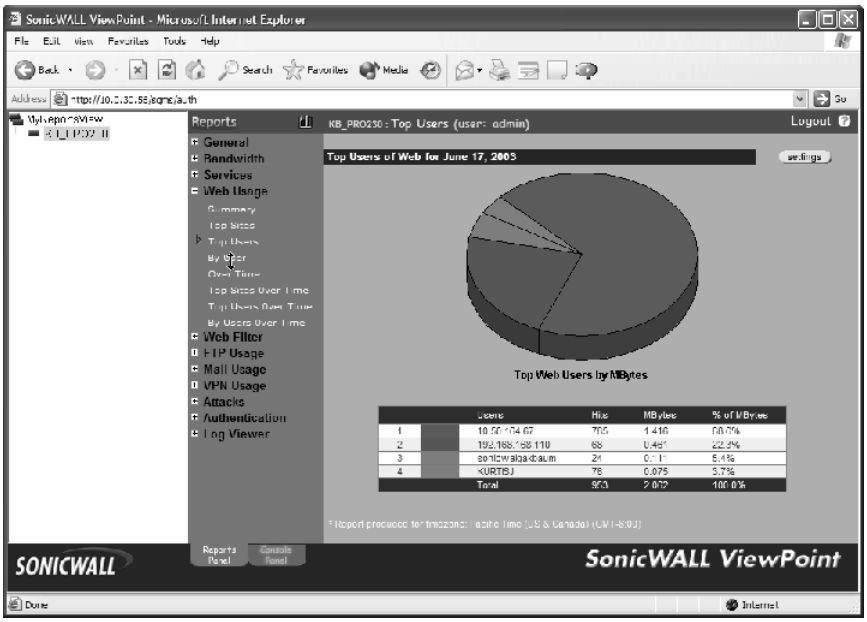
Viewing the Top Users of HTTP Bandwidth

The Top Users report displays the users who used the most HTTP bandwidth on the specified date.

To view the Top Users report, follow these steps:

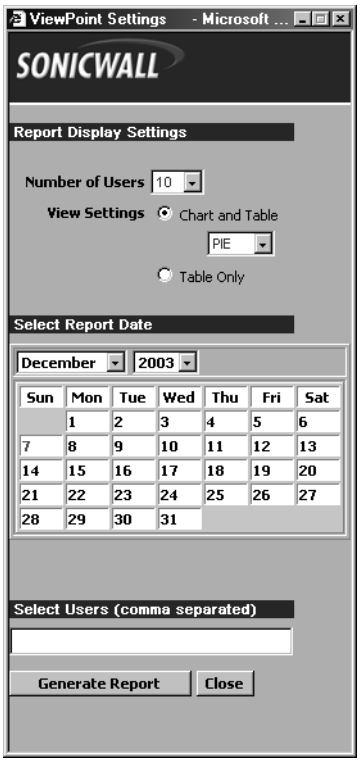
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Web Usage tree and click **Top Users**. The Top Users page opens.



5. The pie chart displays the percentage of bandwidth transferred by each of the top users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Hits**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the day and 200 megabytes was transferred by the top user, the **% of MBytes** field displays 20%.

7. By default, GMS ViewPointshows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The ViewPoint Settings dialog box opens.



8. Select the number of users to display from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day to view.
11. Enter user names to generate reports on specific users. Use commas to separate the names.
12. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

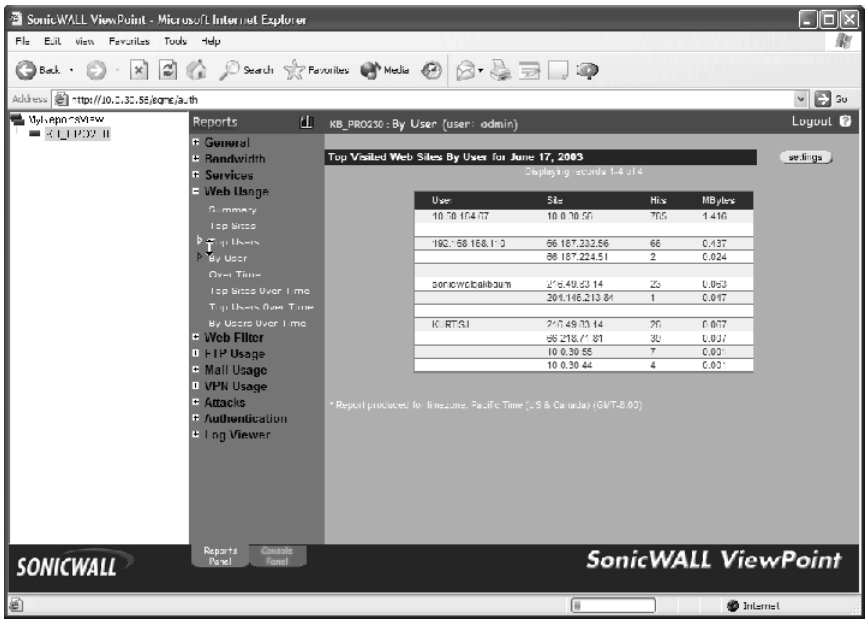
    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing HTTP Bandwidth Usage by User

The By User report displays a list of all users, their top sites, the number of hits to each site, and the amount of data transferred.

To view the By User report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Usage tree and click **By User**. The By User page opens.



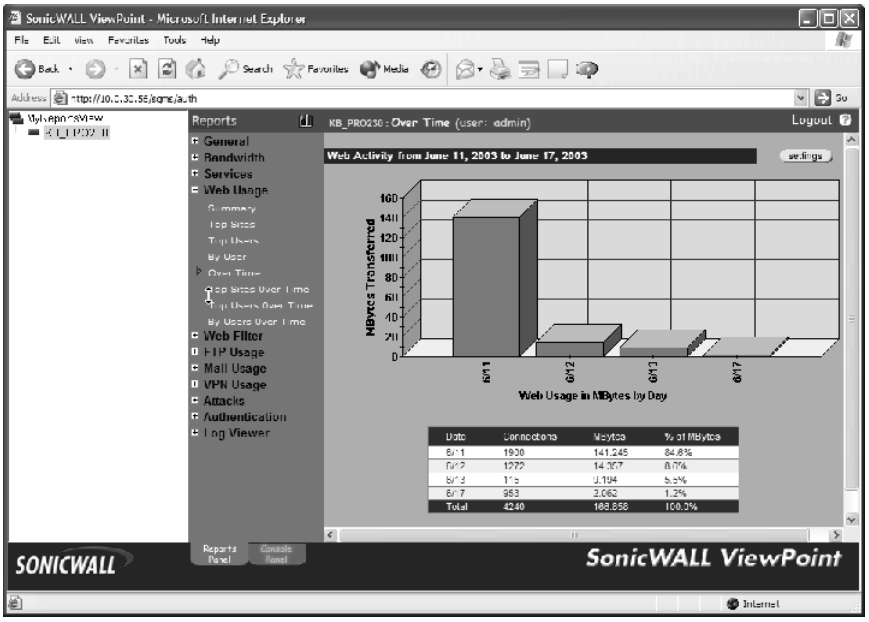
5. The table contains the following information:
   - **User**—the IP address of the user.
   - **Site**—the top five sites visited by the user.
   - **Attempts**—number of hits to each web site visited by the user.
   - **MBytes**—number of megabytes transferred.
6. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.
7. Select the year, month, and day to view.
8. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

Viewing Bandwidth Usage Over Time

The Web Usage Over Time report displays the daily amount of HTTP bandwidth handled by a SonicWALL appliance or group of SonicWALL appliances for the specified time period.

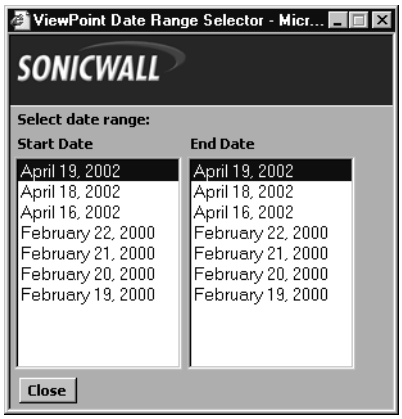
To view the Web Usage Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Web Usage tree and click **Over Time**. The Over Time page opens.



5. The bar graph displays the amount of HTTP bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of connections or hits.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this day, compared to the time period. For example, if 100,000 megabytes of data was transferred during the time period and 25,000 megabytes was transferred on one day, the **% MBytes** field displays 25%.

7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

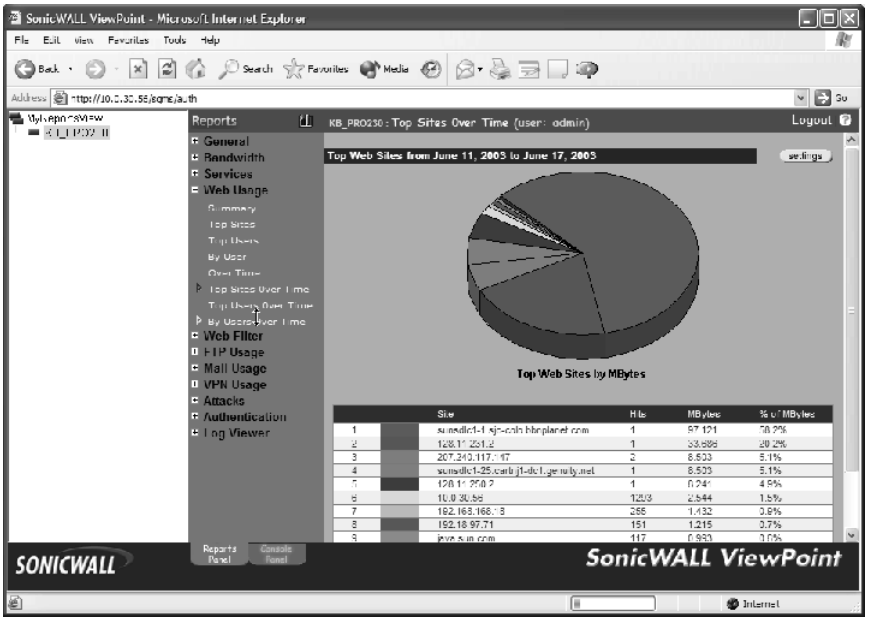
Viewing Top Sites Over Time

The Top Sites Over Time report displays the most visited web sites for the specified time period.

To view the Top Sites Over Time report, follow these steps:

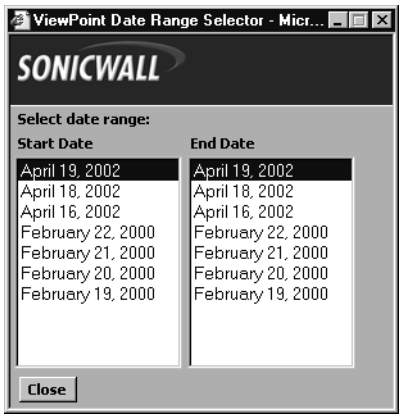
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Web Usage tree and click **Top Sites Over Time**. The Top Sites Over Time page opens.



5. The bar graph displays the amount of HTTP bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Hits**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred between this site, compared to all other HTTP traffic. For example, if 1,000 megabytes of data was transferred during the day and 500 megabytes was transferred between the appliance and Ebay, the **% of MBytes** field displays 50%.

7. To change the date range of the report, click **Settings**. The ViewPoint Settings dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

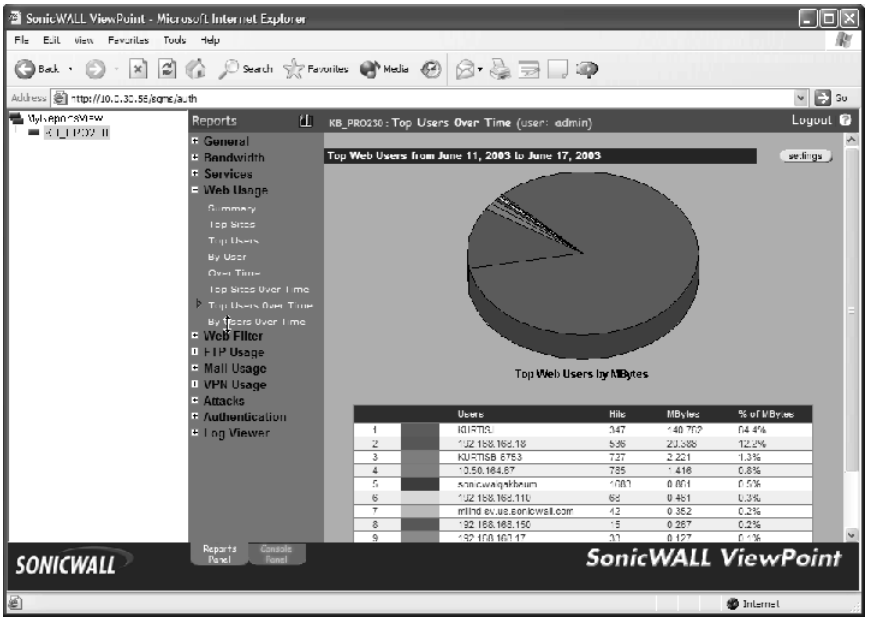
   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing Top Users Over Time

The Top Users Over Time report displays the top users of bandwidth for the specified time period. To view the Top Users Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Web Usage tree and click **Top Users Over Time**. The Top Users Over Time page opens.



5. The graph provides a graphical display of the percentage of bandwidth transferred by each of the top users over the specified time period.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Hits**—number of hits.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 1000 megabytes of data was transferred during the period and 200 megabytes was transferred by the top user, the **% of MBytes** field displays 20%.

7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.

8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

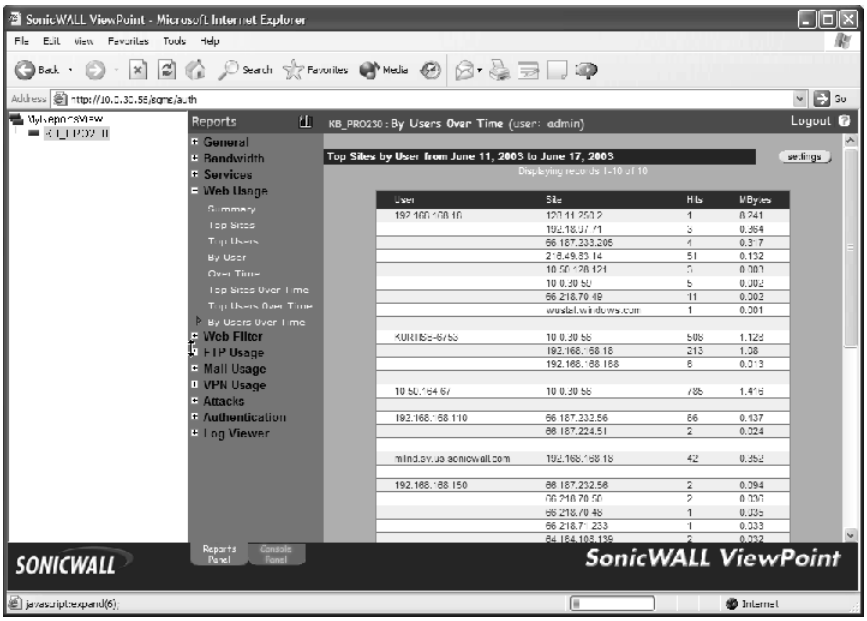
   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing Bandwidth Usage By User Over Time

The By User Over Time report displays a list of all users, their top sites, the number of hits to each site, and the amount of data transferred for the specified time period.

To view the By User Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Usage tree and click **By User Over Time**. The By User Over Time page opens.



5. The bar graph displays the amount of HTTP bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - **User**—the IP address of the user.
   - **Site**—the top five sites visited by the user.
   - **Hits**—number of hits to each web site visited by the user.
   - **MBytes**—number of megabytes transferred.

7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.

8. Select the starting and ending dates to view.
9. Enter user names to generate reports on specific users. Use commas to separate the user names.
10. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing Web Filter Reports

Web filter reports provide information on the number of attempts that users made to access blocked web sites through the selected SonicWALL appliance(s). These reports include web sites blocked by the Content Filter List, customized keyword filtering, and domain name filtering.

Web filter reports can be used to view blocked site access attempts by the hour, day, or over a period of days. Additionally, you can view the users that most frequently attempt to access blocked sites and the most popular blocked sites.

Report Name	Unit Level	Group Level
Web Filter Summary Report	Yes	Yes
Top Filtered Web Sites	Yes	
Top Filtered Web Sites by User	Yes	
Top Filtered Sites by User	Yes	Yes
Top Blocked Web Sites Over Time	Yes	
Top Blocked Web Users Over Time	Yes	
Top Blocked Sites by User Over Time	Yes	

Note: *The single firewall report opens in the firewall's local time. The aggregate multi-firewall report opens in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Note: *Content Filter Categories are now displayed as part of the Web Filter Report.*

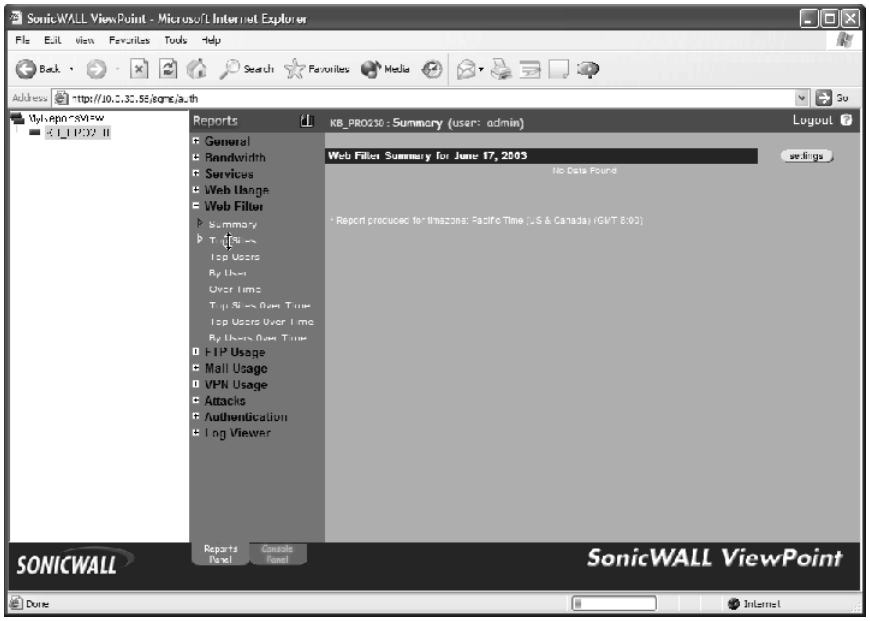
Viewing the Web Filter Summary Report

The Web Filter Summary report contains information on the number of times users attempt to access blocked sites for the specified day.

To view the Web Filter Summary report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the Web Filter tree and click **Summary**. The Summary page opens.



5. The bar graph displays the number of blocked sites that users attempted to access during each hour of the day.
6. The table contains the following information:
   - **Hour**—time when the sample was taken.
   - **Attempts**—number of attempts to access blocked sites.
   - **% of Attempts**—percentage of attempts during this hour, compared to the day. For example, if 100 attempts occurred during the day and 20 attempts occurred at the 12:00 time period, the **% of Attempts** field displays 20%.

Note: *Content Filter Categories are now displayed as part of the Web Filter Report.*

7. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

8. Select the year, month, and day to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

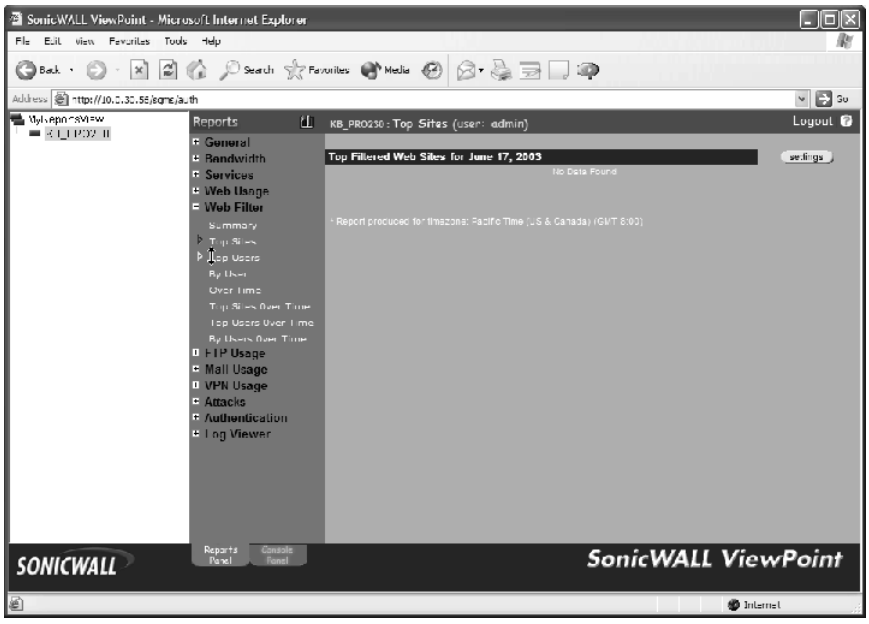
Viewing the Web Filter Top Sites Report

The Web Filter Top Sites report displays the top blocked web sites that users attempted to access on the specified date.

To view the Top Sites report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Web Filter tree and click **Top Sites**. The Top Sites page opens.



5. The graph provides a display of the number of access attempts for each of the top twenty blocked web sites.
6. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Attempts**—number of attempts.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other blocked site attempts. For example, if 500 attempts were made during the day and 100 of those attempts were for www.badsite.com, its **% of Attempts** field displays 20%.

Note: *Content Filter Categories are now displayed as part of the Web Filter Report.*

7. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

8. Select the year, month, and day to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

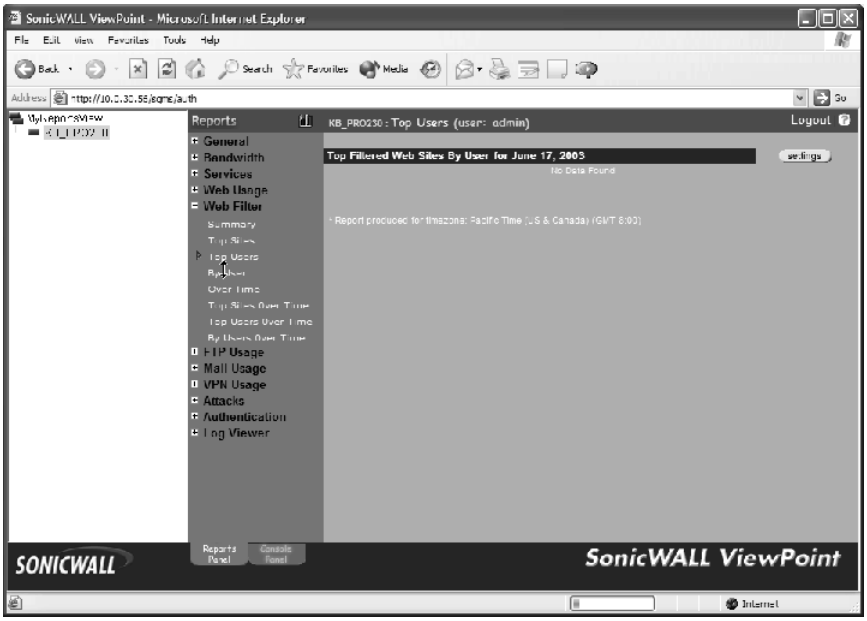
Viewing the Top Users that Try to Access Blocked Sites

The Web Filter Top Users report displays the users who made the most attempts to access blocked sites on the specified date.

To view the Top Users report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Web Filter tree and click **Top Users**. The Top Users page opens.



5. The pie chart displays the top users with the most blocked site attempts.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Attempts**—number of attempts.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other user attempts. For example, if 500 attempts were made during the day and 250 of those attempts were made by a single user, the **% of Attempts** field displays 50%.

7. By default, ViewPoint shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The ViewPoint Settings dialog box opens.

8. Select the number of users to display from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day to view.
11. Enter user names to generate reports on specific users. Use commas to separate the user names.
12. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

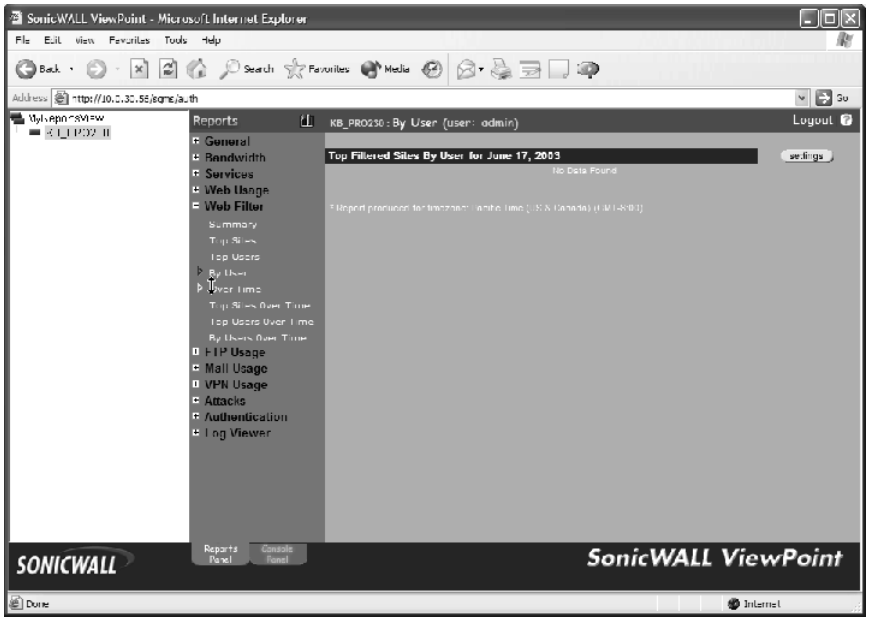
Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing the Top Blocked Sites for Each User

The Web Filter By User report displays the top blocked web sites that each user attempted to access on the specified date.

To view the Web Filter By User report, follow these steps:

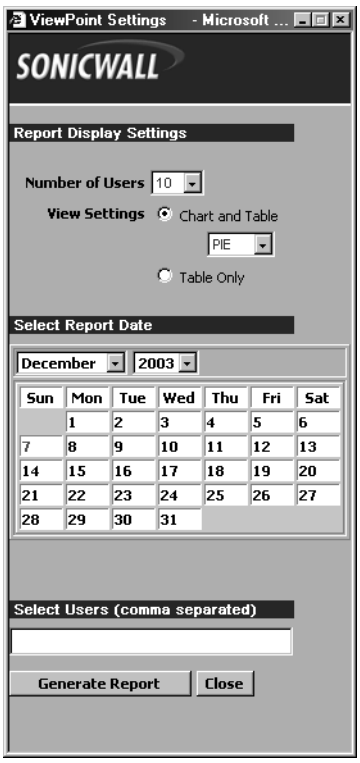
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Filter tree and click **By User**. The By User page opens.



5. The table contains the following information:
   - **User**—the IP address of the user.
   - **Site**—the top five sites visited by the user.
   - **Attempts**—number of attempts the user made to access each web site.

Note: *Content Filter Categories are now displayed as part of the Web Filter Report.*

6. By default, SonicWALL ViewPoint shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The ViewPoint Settings dialog box opens.



7. Select the number of users to display from the **Number of Users** list box.
8. Select the type of chart from the **Chart Type** list box.
9. Select the year, month, and day to view.
10. Enter user names to generate reports on specific users. Use commas to separate the user names.
11. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

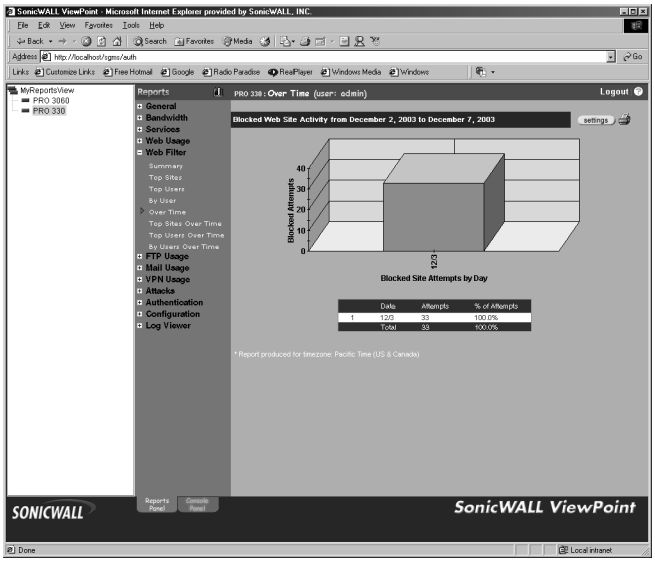
    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing Blocked Site Attempts Over Time

The Web Filter Over Time report displays the number of attempts that were made to access blocked web sites for the specified time period.

To view the Web Filter Over Time report, follow these steps:

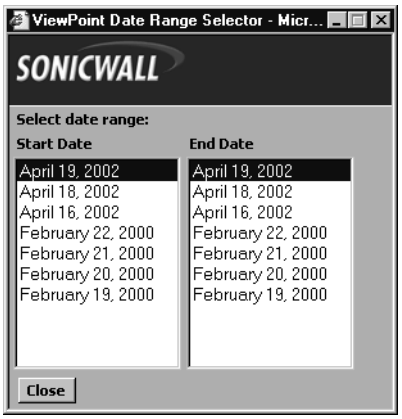
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Web Filter tree and click **Over Time**. The Over Time page opens.



5. The bar graph displays the number of attempts that were made to access blocked web sites during each day of the specified time period.
6. The table contains the following information:
   - **Date**—day when the sample was taken.
   - **Attempts**—number of attempts to access blocked web sites.
   - **% of Attempts**—percentage of attempts to access the blocked site on the day, compared to the time period. For example, if 5,000 attempts were made during the time period and 500 were made on one day, its **% of Attempts** field displays 10%.

Note: *Content Filter Categories are now displayed as part of the Web Filter Report.*

7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

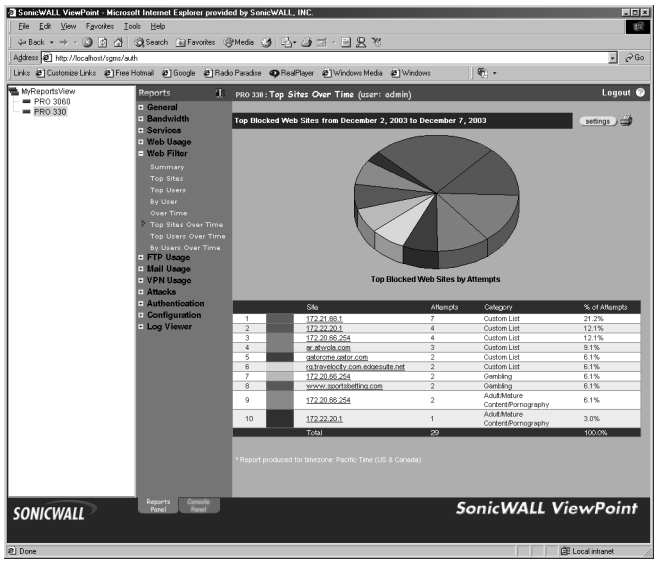
Viewing the Top Blocked Site Attempts Over Time

The Top Sites Over Time report displays the top blocked web sites for the specified time period.

To view the Web Filter Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

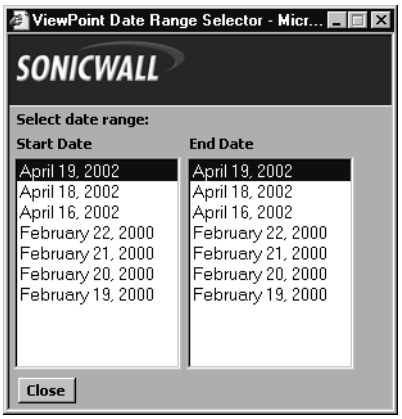
4. Expand the Web Filter tree and click **Top Sites Over Time**. The Top Sites Over Time page opens.



5. The graph displays the number of access attempts for each of the top blocked web sites during the specified time period.
6. The table contains the following information:
   - **Site**—URL or IP address of the site.
   - **Attempts**—number of attempts.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other blocked site attempts. For example, if 500 attempts were made during the period and 100 of those attempts were for www.badsite.com, its **% of Attempts** field displays 20%.

Note: *Content Filter Categories are now displayed as part of the Web Filter Report.*

7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

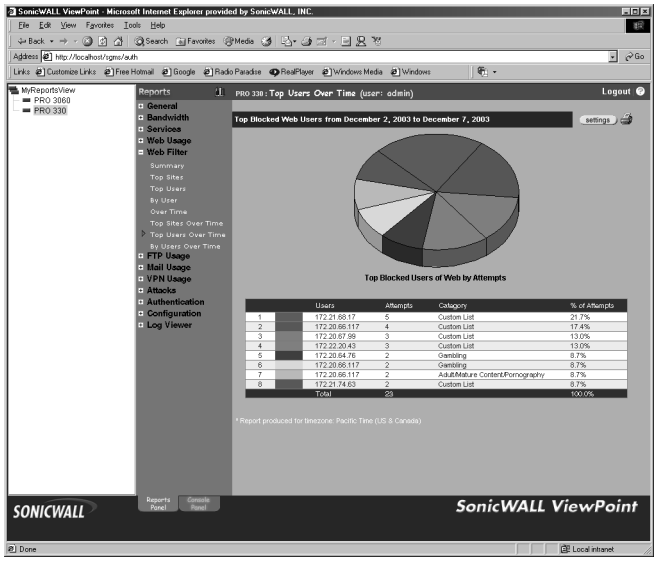
Viewing the Top Blocked Site Users Over Time

The Web Filter Top Users Over Time report displays the users who made the most attempts to access blocked sites during the specified time period.

To view the Top Users Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Web Filter tree and click **Top Users Over Time**. The Top Users Over Time page opens.



5. The pie chart displays the top users with the most blocked site attempts.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Attempts**—number of attempts.
   - **% of Attempts**—percentage of attempts to access the blocked site, compared to all other user attempts. For example, if 500 attempts were made during the period and 250 of those attempts were made by a single user, his **% of Attempts** field displays 50%.

Note: *Content Filter Categories are now displayed as part of the Web Filter Report.*

7. To change the date range of the report, click **Settings**. The ViewPoint Settings dialog box opens.

8. Select the starting and ending dates to view.
9. Enter user names to generate reports on specific users. Use commas to separate the user names.
10. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

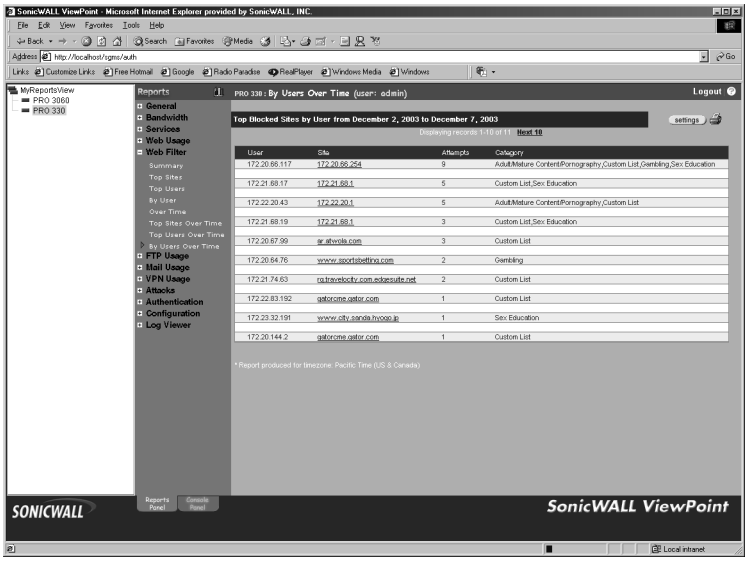
    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing the Top Blocked Sites for Each User Over Time

The Web Filter By User report displays the top blocked web sites that each user attempted to access during the specified time period.

To view the By User Over Time report, follow these steps:

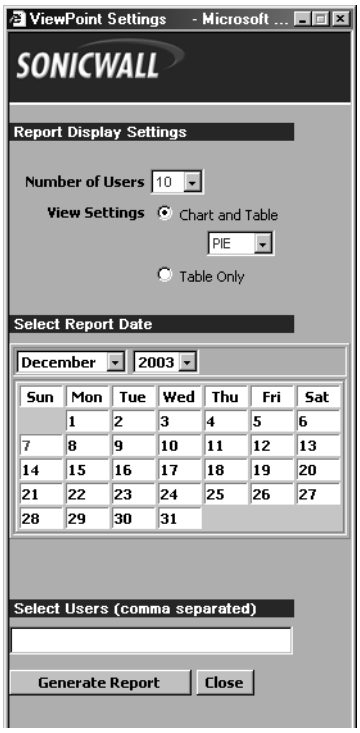
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the Web Filter tree and click **By User Over Time**. The By User Over Time page opens.



5. The table contains the following information:
   - **User**—the IP address of the user.
   - **Site**—the top five sites visited by the user.
   - **Attempts**—number of attempts the user made to access each web site.

Note: *Content Filter Categories are now displayed as part of the Web Filter Report.*

6. To change the date range of the report, click **Settings**. The ViewPoint Settings dialog box opens.



7. Select the starting and ending dates to view.
8. Enter user names to generate reports on specific users. Use commas to separate the user names.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing File Transfer Protocol Reports

FTP usage reports provide information on the amount of FTP usage that occurs through the selected SonicWALL appliance(s).

FTP usage reports can be used to view FTP bandwidth usage by the hour, day, or over a period of days. Additionally, you can view the top users of FTP bandwidth.

General bandwidth reports do not always provide a complete picture of network bandwidth usage. If a large amount of FTP traffic occurs during peak times, you might need more bandwidth, you might need to upgrade network equipment, or you might ask employees to use compression or transfer large files during non-peak times..

Report Name	Unit Level	Group Level
FTP Usage Summary	Yes	Yes
Top Users of FTP	Yes	
FTP Activity Over Time	Yes	Yes
Top Users of FTP Over Time	Yes	

Note: *The single firewall report opens in the firewall's local time. The aggregate multi-firewall report opens in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

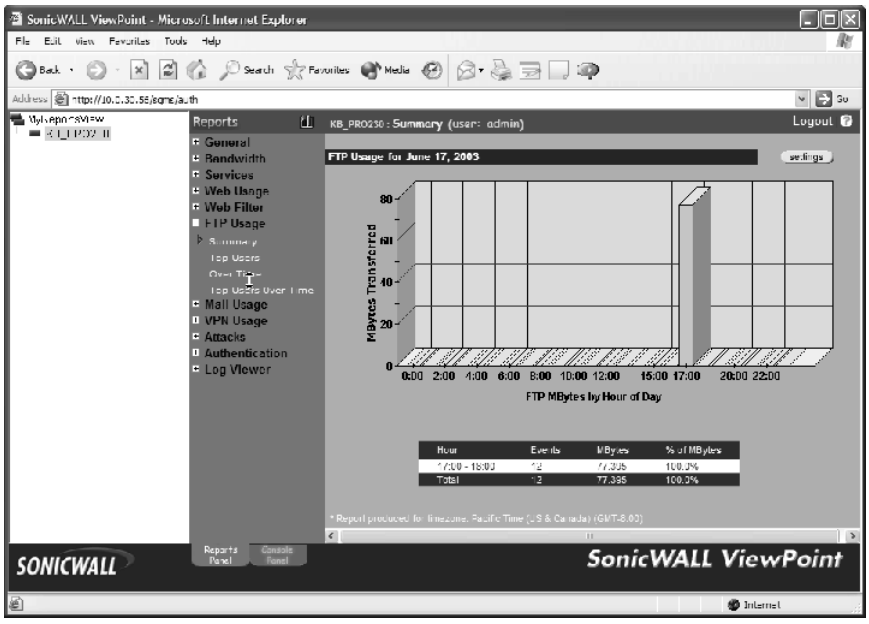
Viewing the FTP Summary Report

The FTP Summary report contains information on the amount of FTP bandwidth handled by a SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the FTP Summary report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the FTP Usage tree and click **Summary**. The Summary page opens.

.



5. The bar graph displays the amount of FTP bandwidth transferred during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of FTP events.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this hour, compared to the day. For example, if 1000 megabytes of FTP data was transferred during the day and 100 megabytes was transferred at the 12:00 time period, the **% of MBytes** field displays 10%.

7. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

8. Select the year, month, and day to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

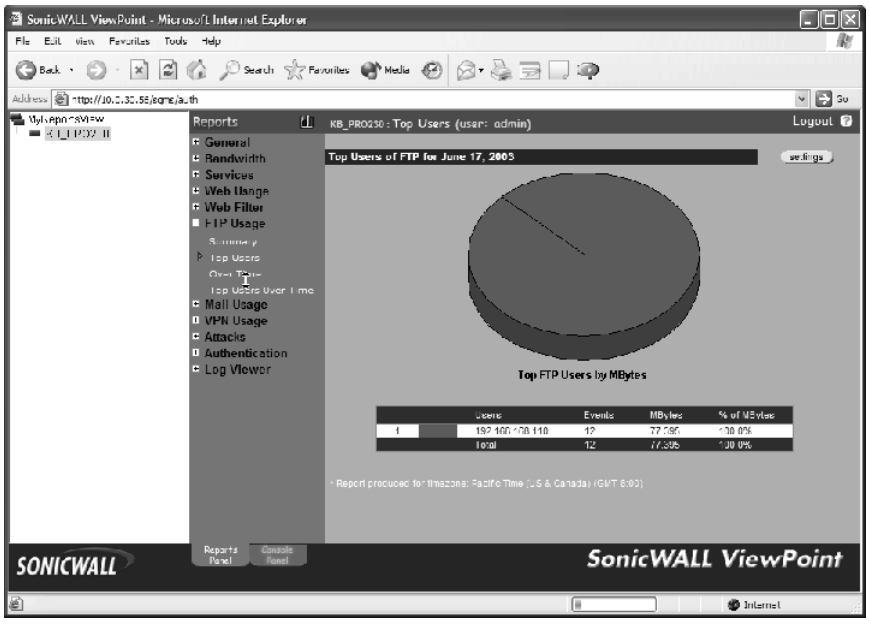
Viewing the Top Users of FTP Bandwidth

The Top Users report displays the users who used the most FTP bandwidth on the specified date.

To view the Top Users report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the FTP Usage tree and click **Top Users**. The Top Users page opens.



5. The pie chart displays the percentage of bandwidth used by each user.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—number of FTP Events.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if ten megabytes of data was transferred during the day and two megabytes was transferred by the top user, the **% of Mbytes** field displays 20%.

7. By default, SonicWALL ViewPoint shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The ViewPoint Settings dialog box opens.

8. Select the number of users to display from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day to view.
11. Enter user names to generate reports on specific users. Use commas to separate the user names.
12. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

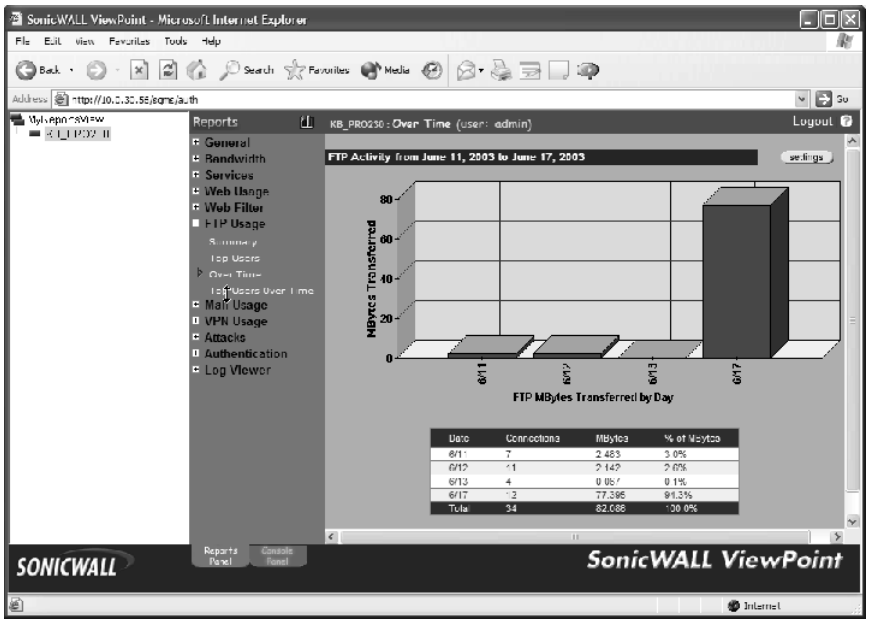
Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing FTP Bandwidth Usage Over Time

The FTP Usage Over Time report displays the daily amount of FTP bandwidth handled by a SonicWALL appliance or group of SonicWALL appliances for the specified time period.

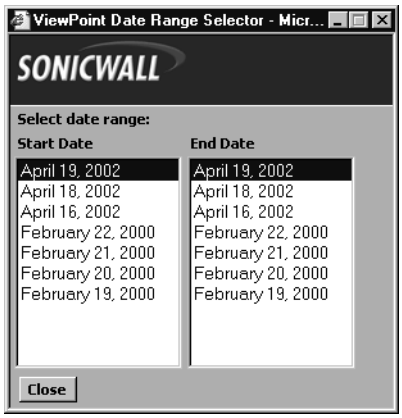
To view the FTP Usage Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the FTP Usage tree and click **Over Time**. The Over Time page opens.



5. The bar graph displays the amount of FTP bandwidth transferred during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of FTP connections.
   - **MBytes**—number of megabytes transferred.
   - **% of Usage**—percentage of megabytes transferred during this day, compared to the time period. For example, if 10,000 megabytes of FTP data was transferred during the time period and 2,500 megabytes of FTP data was transferred on one day, the **% of Usage** field displays 25%.

7. To change the date range of the report, click **Settings**. The ViewPoint Settings dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

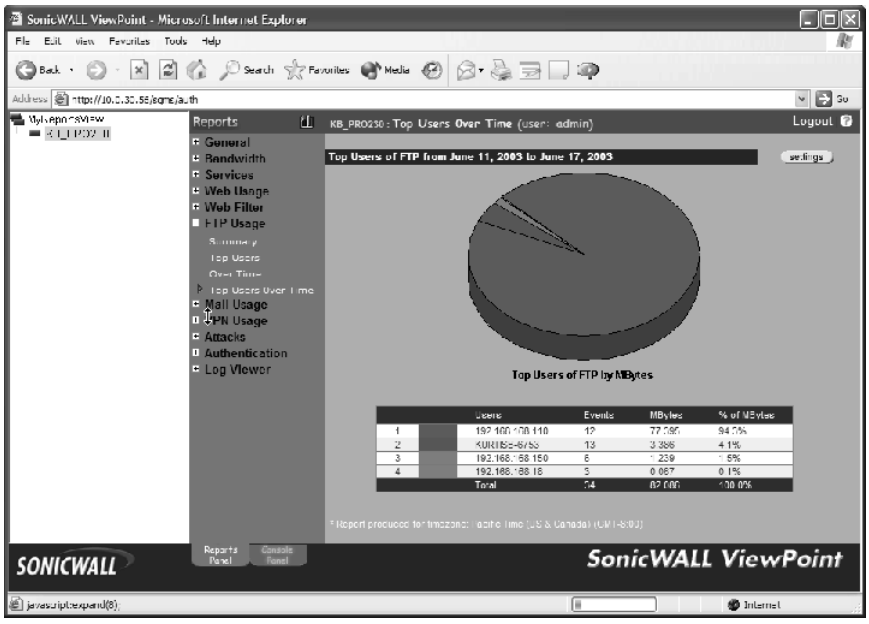
Viewing the Top Users of FTP Bandwidth Over Time

The Top Users Over Time report displays the users who used the most FTP bandwidth for the specified time period.

To view the Top Users Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the FTP Usage tree and click **Top Users Over Time**. The Top Users Over Time page opens.



5. The pie chart displays the percentage of bandwidth used by each user.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—number of FTP Events.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if ten megabytes of data was transferred during the period and two megabytes was transferred by the top user, the **% of MBytes** field displays 20%.

7. To change the date range of the report, click **Settings**. The ViewPoint Settings dialog box opens.

8. Select the starting and ending dates to view.
9. Enter user names to generate reports on specific users. Use commas to separate the user names.
10. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing Mail Usage Reports

Mail usage reports provide information on the amount of mail usage that occurs through the selected SonicWALL appliance(s).

Mail usage reports can be used to view mail bandwidth usage by the hour, day, or over a period of days. Additionally, you can view the top users of mail bandwidth.

Note: *Mail usage reports include SMTP, POP3, and IMAP traffic.*

General bandwidth reports do not always provide a complete picture of network bandwidth usage. If a large amount of mail traffic occurs during peak times, you might want to take some of the following actions:

- Add bandwidth
- Upgrade network equipment
- Ask employees to use compression or transfer large files during non-peak times
- Ask employees to place large files on an FTP site rather than sending them as mail attachments.

Report Name	Unit Level	Group Level
Mail Usage Summary	Yes	Yes
Top Mail Users	Yes	
Mail Usage Over Time	Yes	Yes
Top Users of Mail Over Time	Yes	

Note: *The single firewall report opens in the firewall's local time. The aggregate multi-firewall report opens in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

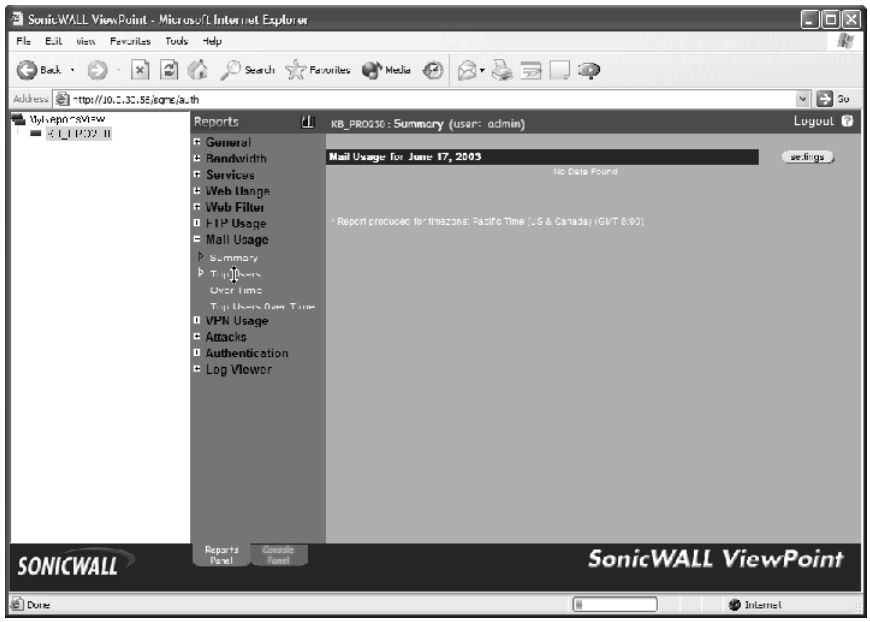
Viewing the Mail Usage Summary Report

The Mail Usage Summary report contains information on the amount of mail handled by a SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the Mail Usage Summary report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the Mail Usage tree and click **Summary**. The Summary page opens.



5. The bar graph displays the amount of mail sent and received during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Events**—number of mail events.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred during this hour, compared to the day. For example, if 10,000 megabytes of mail was transferred during the day and 1,000 megabytes was transferred at the 12:00 time period, the **% of MBytes** field displays 10%.

7. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

8. Select the year, month, and day to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

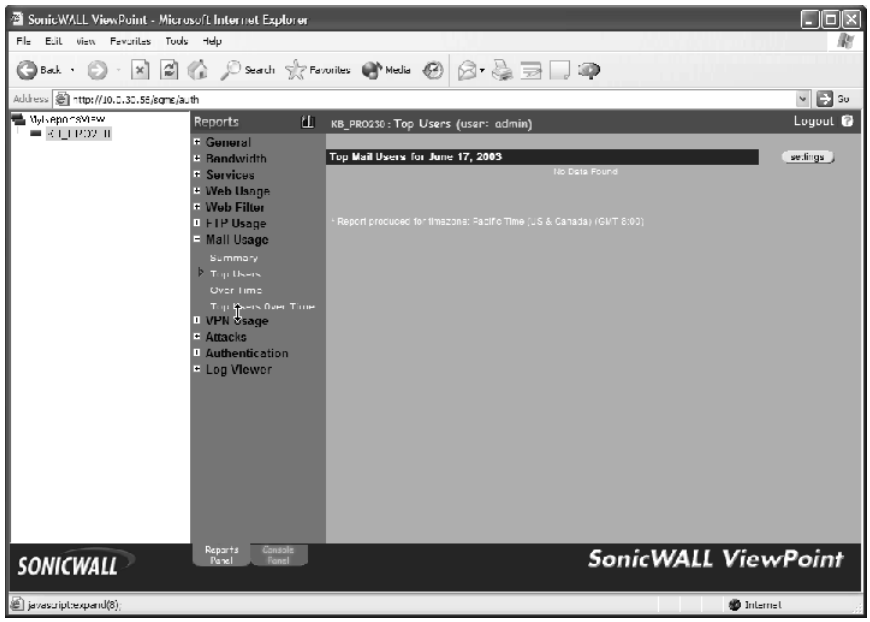
Viewing the Top Users of Mail Bandwidth

The Top Users report displays the users who sent and received the most mail on the specified date.

To view the Top Users report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Mail Usage tree and click **Top Users**. The Top Users page opens.



5. The pie chart displays the percentage of mail sent and received by the top mail users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—number of mail messages sent and received.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 10000 megabytes of data was transferred during the day and 2000 megabytes was transferred by the top user, the **% of MBytes** field displays 20%.

7. By default, SonicWALL ViewPoint shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The ViewPoint Settings dialog box opens.

8. Select the number of users to display from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day to view.
11. Enter user names to generate reports on specific users. Use commas to separate the user names.
12. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

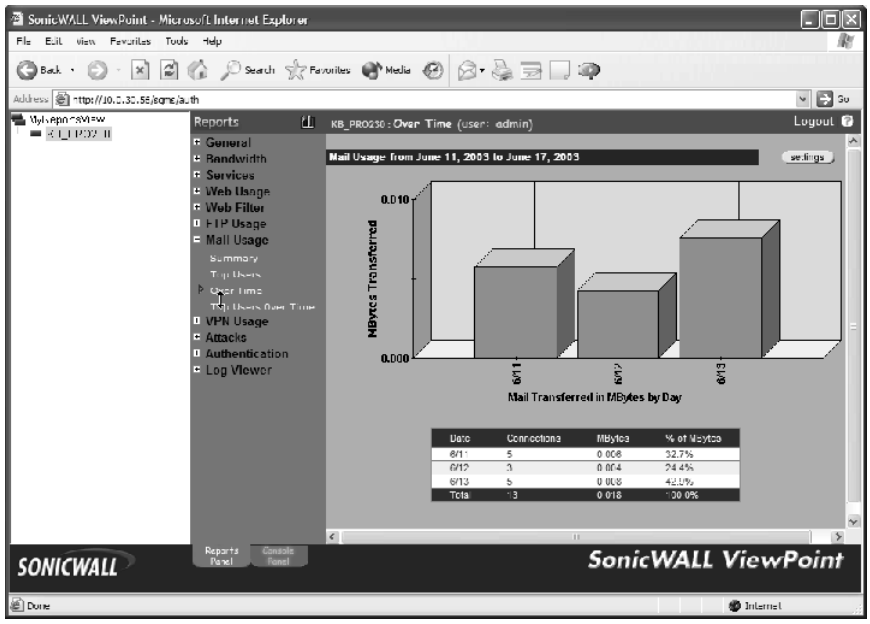
Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing Mail Usage Over Time

The Mail Usage Over Time report displays the daily amount of mail handled by a SonicWALL appliance or group of SonicWALL appliances for the specified time period.

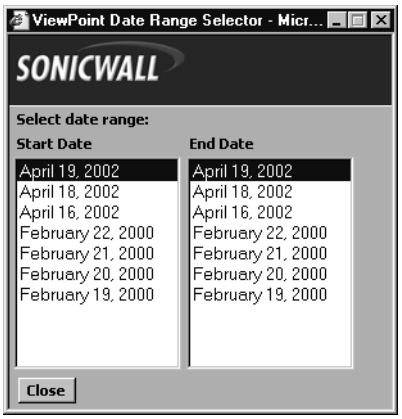
To view the Mail Usage Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the Mail Usage tree and click **Over Time**. The Over Time page opens.



5. The bar graph displays the amount of mail sent and received during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of mail messages.
   - **MBytes**—number of megabytes transferred.
   - **% of Usage**—percentage of megabytes transferred during this day, compared to the time period. For example, if 10,000 megabytes of mail was transferred during the time period and 2,500 megabytes of mail was transferred on one day, the **% of Usage** field displays 25%.

7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

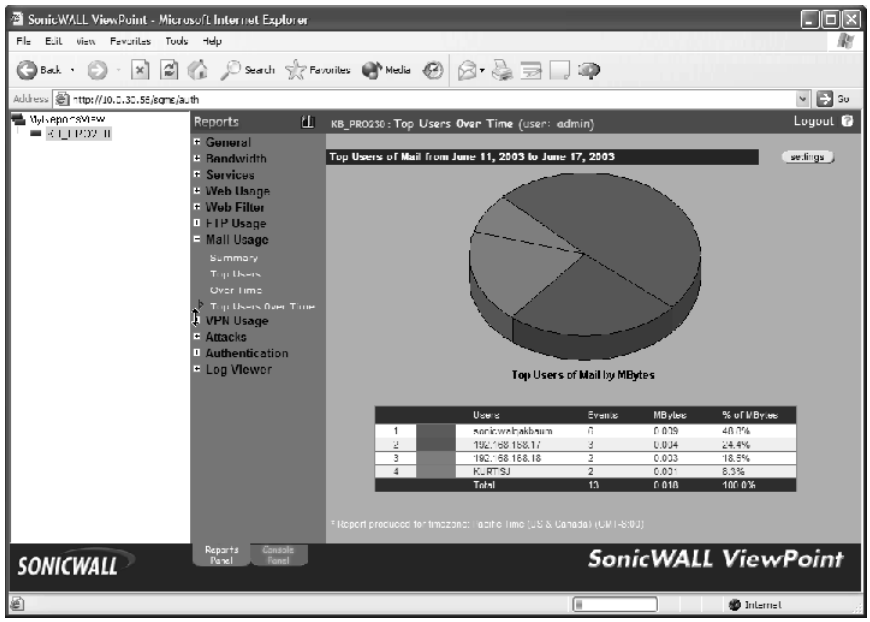
Viewing the Top Users of Mail Bandwidth Over Time

The Top Users Over Time report displays the users who sent and received the most mail during the specified time period.

To view the Top Users Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Mail Usage tree and click **Top Users Over Time**. The Top Users Over Time page opens.



5. The pie chart displays the percentage of mail sent and received by the top mail users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Events**—number of mail messages sent and received.
   - **MBytes**—number of megabytes transferred.
   - **% of MBytes**—percentage of megabytes transferred by this user, compared to all users. For example, if 10000 megabytes of data was transferred during the period and 2000 megabytes was transferred by the top user, the **% of MBytes** field displays 20%.

7. To change the date range of the report, click **Settings**. The ViewPoint Settings dialog box opens.

8. Select the starting and ending dates to view.
9. Enter user names to generate reports on specific users. Use commas to separate the user names.
10. When you are finished, click **Close**.GMS ViewPointdisplays the report for the selected date range.

Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing VPN Usage Reports

VPN Usage reports provide information on the amount of VPN usage that occurs through the selected SonicWALL appliance(s).

VPN Usage reports can be used to view VPN usage by the hour, day, or over a period of days. Additionally, you can view the top users of VPN.

General bandwidth reports do not always provide a complete picture of network bandwidth usage. If a large amount of VPN traffic occurs, you might need to add bandwidth, upgrade network equipment, or reconfigure the VPN network.

Report Name	Unit Level	Group Level
VPN Usage Summary	Yes	Yes
Top Users of VPN	Yes	
VPN Activity Over Time	Yes	Yes
Top Users of VPN Over Time	Yes	

Note: *The single firewall report opens in the firewall's local time. The aggregate multi-firewall report opens in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

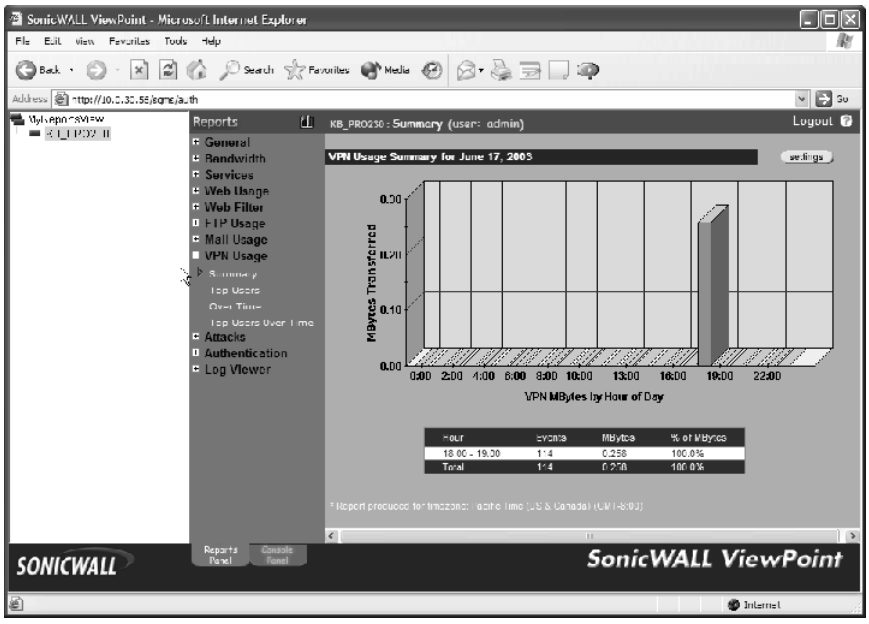
Viewing the VPN Usage Summary Report

The VPN Usage Summary report contains information on the number of VPN connections made through a
SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the VPN Usage Summary report, follow these steps:

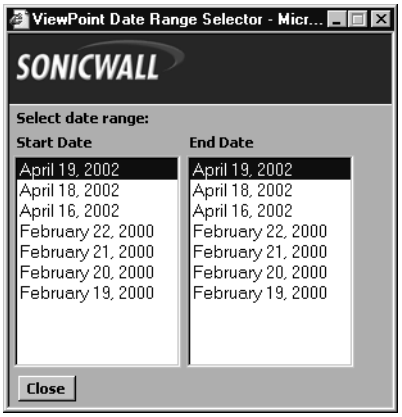
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the VPN Usage tree and click **Summary**. The Summary page opens.



5. The bar graph displays the number of VPN connections made during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Connections**—number of VPN connections.
   - **% of Connections**—percentage of VPN connections during this hour, compared to the day. For example, if 10,000 connections occurred during the day and 1,000 connections occurred during the 2:00 time period, the **% of Connections** field displays 10%.

7. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.



8. Select the year, month, and day to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

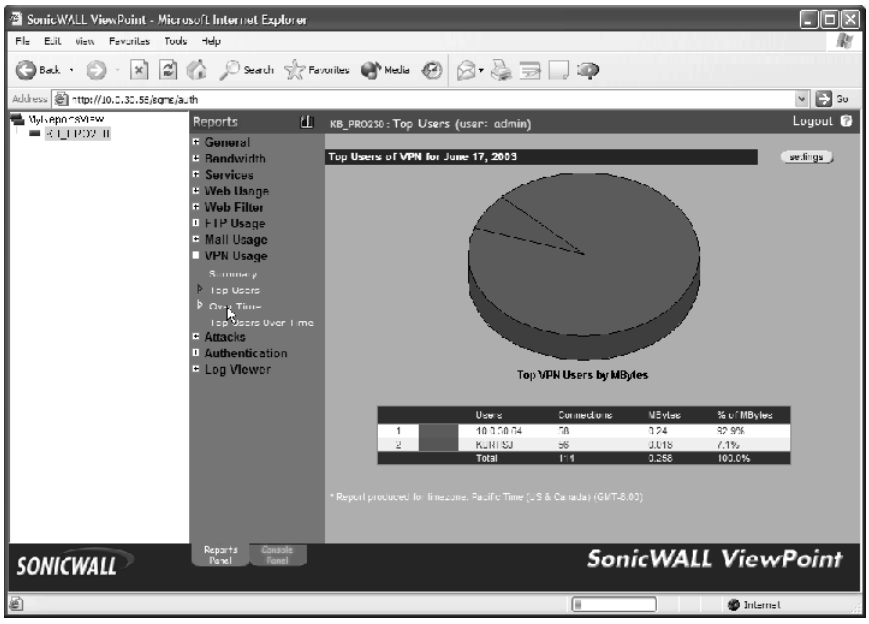
Viewing the Top VPN Users

The Top Users report displays the users who made the most VPN connections on the specified date.

To view the Top Users report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the VPN Usage tree and click **Top Users**. The Top Users page opens.



5. The pie chart displays the VPN connections for the top VPN users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of VPN connections.
   - **% of Connections**—percentage of VPN connections made by this user, compared to all other users. For example, if 10,000 connections occurred during the day and 1,000 connections were made by one user, the **% of Connections** field displays 10%.

7. By default, SonicWALL ViewPoint shows today's report, a pie chart, and the ten top users. To change these settings, click **Settings**. The ViewPoint Settings dialog box opens.

8. Select the number of users to display from the **Number of Users** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day to view.
11. Enter user names to generate reports on specific users. Use commas to separate the user names.
12. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

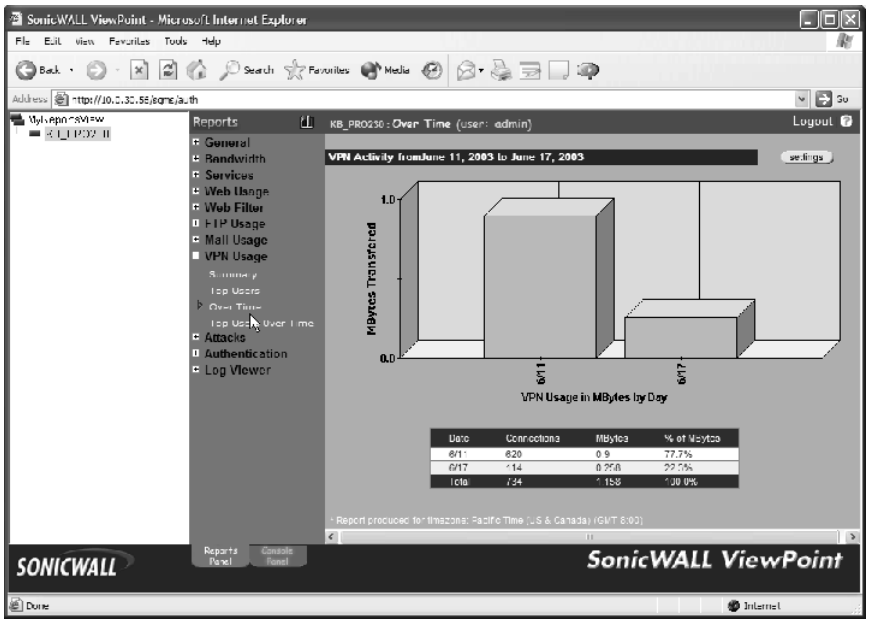
Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing VPN Usage Over Time

The VPN Usage Over Time report displays the daily number of VPN connections made through a SonicWALL appliance or group of SonicWALL appliances during the specified time period.

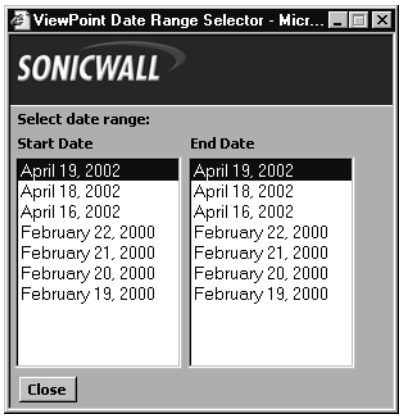
To view the VPN Usage Over Time report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the VPN Usage tree and click **Over Time**. The Over Time page opens.



5. The bar graph displays the number of VPN connections made during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Connections**—number of connections.
   - **MBytes**—number of megabytes transferred.
   - **% of Usage**—percentage of kilobytes transferred during this day, compared to the time period. For example, if 10,000 kilobytes of mail was transferred during the time period and 2,500 kilobytes of mail was transferred on one day, the **% of Usage** field displays 25%.

7. To change the date range of the report, click **Settings**. The ViewPoint Settings dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

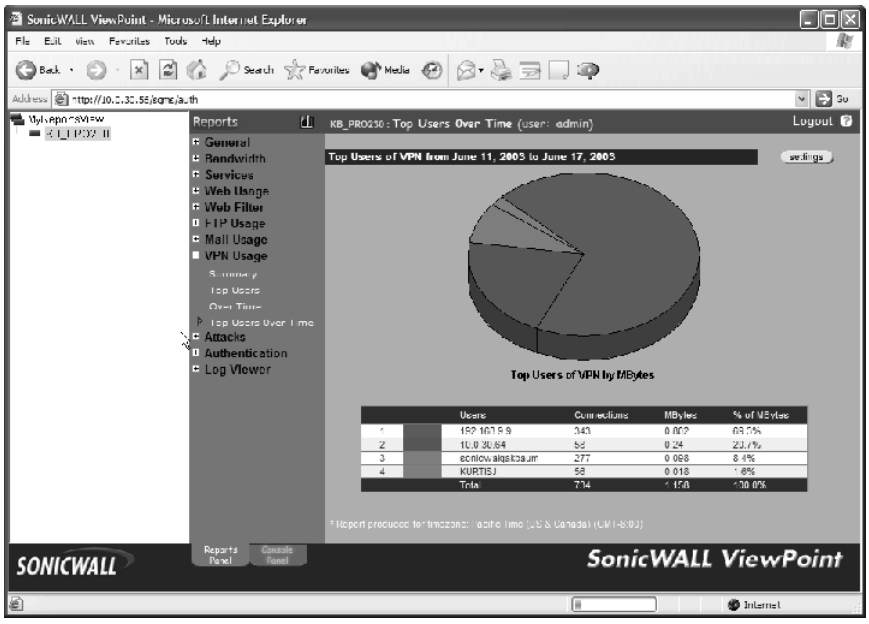
Viewing the Top VPN Users Over Time

The Top Users report displays the users who made the most VPN connections for the specified time period.

To view the Top Users report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the VPN Usage tree and click **Top Users Over Time**. The Top Users Over Time page opens.



5. The pie chart displays the VPN connections for the top VPN users.
6. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—number of VPN connections.
   - **% of Connections**—percentage of VPN connections made by this user, compared to all other users. For example, if 10,000 connections occurred during the period and 1,000 connections were made by one user, the **% of Connections** field displays 10%.

7. To change the date range of the report, click **Settings**. The ViewPoint Settings dialog box opens.

8. Select the starting and ending dates to view.
9. Enter user names to generate reports on specific users. Use commas to separate the user names.
10. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

Viewing Attack Reports

Attack reports show the number of attacks that were directed at or through the selected SonicWALL appliance(s). These include denial of service attacks, intrusions, probes, and all other malicious activity directed at the SonicWALL appliance or computers on the LAN or DMZ.

Note: *The single firewall report opens in the firewall's local time. The aggregate multi-firewall report opens in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view a summary of the attacks, see "Viewing the Attack Summary Report" on page 128.
- To view the attacks by attack category, see "Viewing the Attacks by Category" on page 130.
- To view the attacks by source IP address, see "Viewing the Attacks by Source" on page 132.
- To view a summary of the errors and exceptions, see "Viewing the Errors and Exceptions Report" on page 134.
- To view attacks over a period of time, see "Viewing Attack Reports Over Time" on page 136.
- To view errors and exceptions over a period of time, see "Viewing Errors Over Time" on page 138.

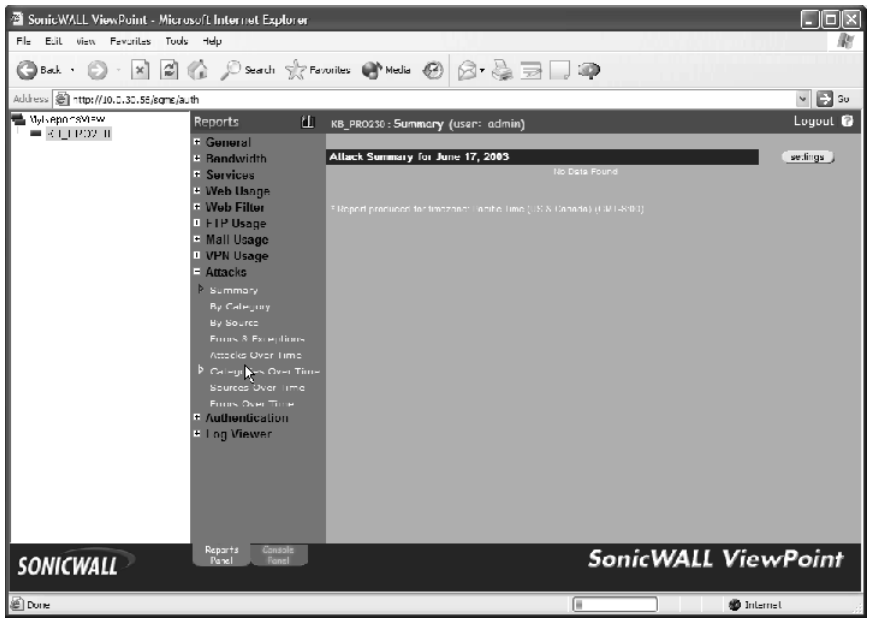
Viewing the Attack Summary Report

The Attack Summary report contains information on the number of attacks attempted on a SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the Attack Summary report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the Attacks tree and click **Summary**. The Summary page opens.



5. The bar graph displays the number of attacks attempted during each hour of the day. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Attacks**—number of attack attempts.
   - **% of Attacks**—percentage of attacks during this hour, compared to the day. For example, if 1,000 attacks occurred during the day and 100 attacks occurred during the 2:00 time period, the **% of Attacks** field displays 10%.

6. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

7. Select the year, month, and day to view.
8. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

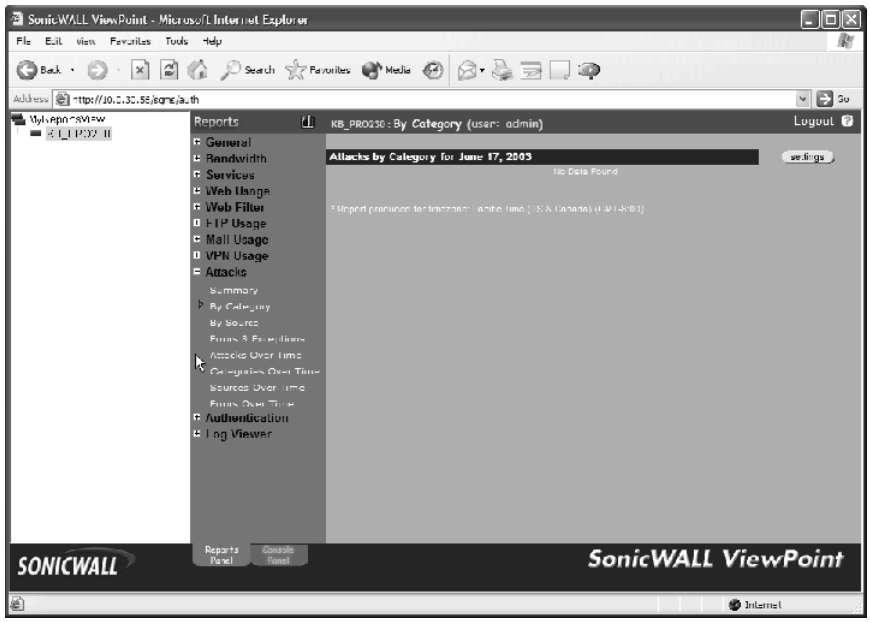
Viewing the Attacks by Category

The **Attacks by Category** report displays the attacks that occurred on the specified date, sorted by category.

To view the **Attacks by Category** report, follow these steps:

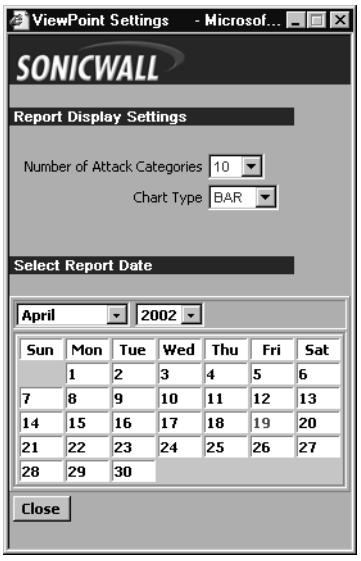
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the **Attacks** tree and click **By Category**. The By Category page opens.



5. The pie chart displays the percentage of each type of attack.
6. The table contains the following information:
   - **Type**—the type of attack.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of this type of attack, compared to all other attack types. For example, if 5,000 attacks occurred during the day and the IP Spoof makes up 500 of the attacks, its **% of Attacks** field displays 10%.

7. By default, SonicWALL ViewPoint shows today's report, a pie chart, and the ten top categories. To change these settings, click **Settings**. The ViewPoint Settings dialog box opens.



8. Select the number of categories to display from the **Number of Categories** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day to view.
11. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

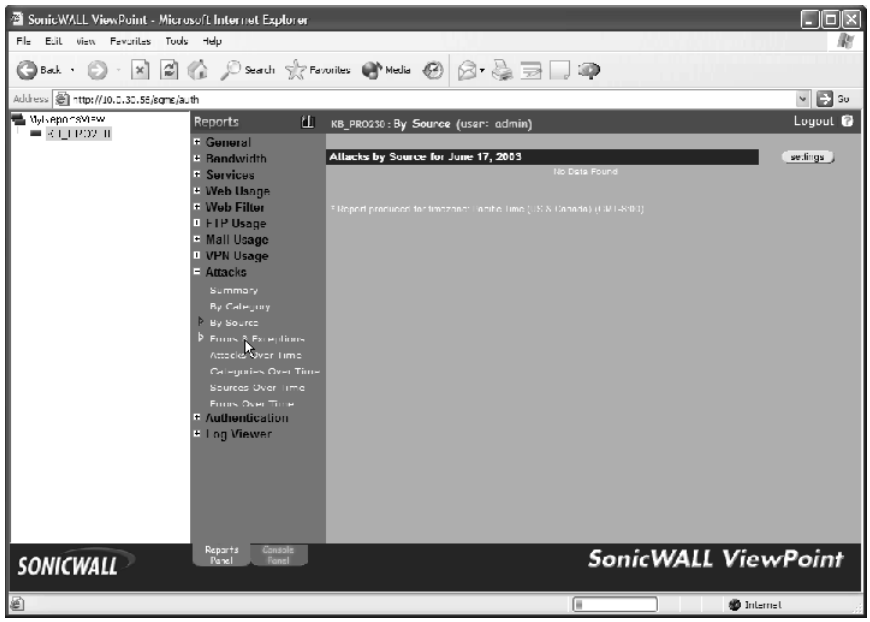
Viewing the Attacks by Source

The **Attacks by Source** report displays the top sources of attacks.

To view the **Attacks by Source** report, follow these steps:

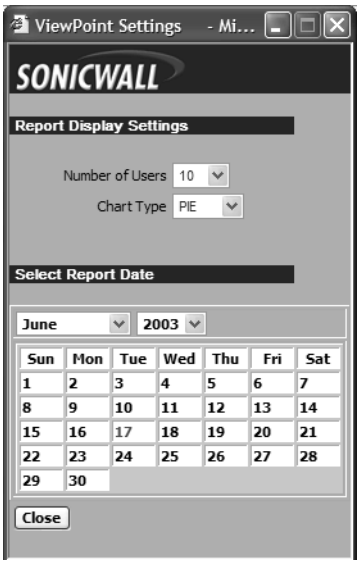
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the Attacks tree and click **By Source**. The By Source page opens.



5. The pie chart displays the percentage of each source of attack.
6. The table contains the following information:
   - **Source**—the source of the attack.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of attacks from this source, compared to all other sources. For example, if 1,000 attacks occurred during the day and 500 attacks came from one source, its **% of Attacks** field displays 50%.

7. By default, SonicWALL ViewPoint shows today's report, a pie chart, and the ten top sources. To change these settings, click **Settings**. The **ViewPoint Settings** dialog box opens.


ViewPoint Settings - Mi...
SONICWALL
Report Display Settings
Number of Users 10
Chart Type PIE
Select Report Date
June 2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

8. Select the number of sources to display from the **Number of Sources** list box.
9. Select the type of chart from the **Chart Type** list box.
10. Select the year, month, and day to view.
11. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

    Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

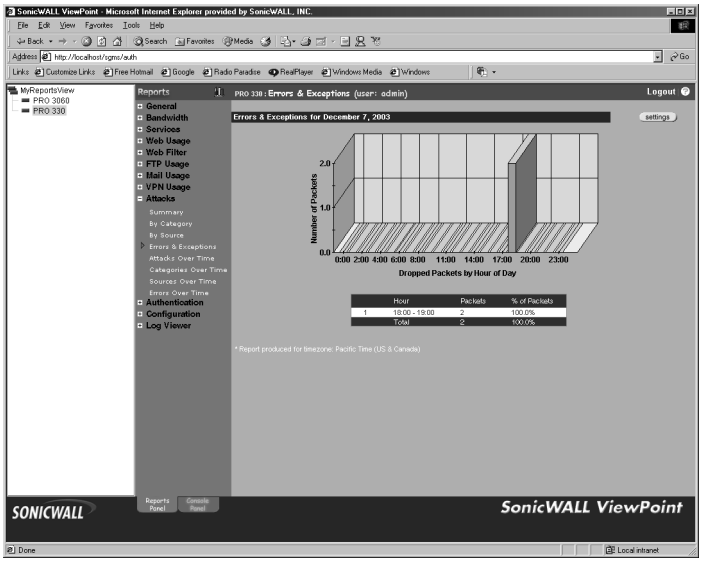
Viewing the Errors and Exceptions Report

The Errors and Exceptions Summary report contains information on the number of dropped packets on a SonicWALL appliance or group of SonicWALL appliances during the specified day.

To view the Errors and Exceptions report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the Attacks tree and click **Errors & Exceptions**. The Errors & Exceptions page opens.



5. The bar graph displays the packets that were dropped during each hour of the day.
6. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Packets**—number of dropped packets.
   - **% of Packets**—percentage of packets dropped during this hour, compared to the day. For example, if 1,000 packets were dropped during the day and 100 packets were dropped during the 1:00 time period, the **% of Packets** field displays 10%.

7. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

8. Select the year, month, and day to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

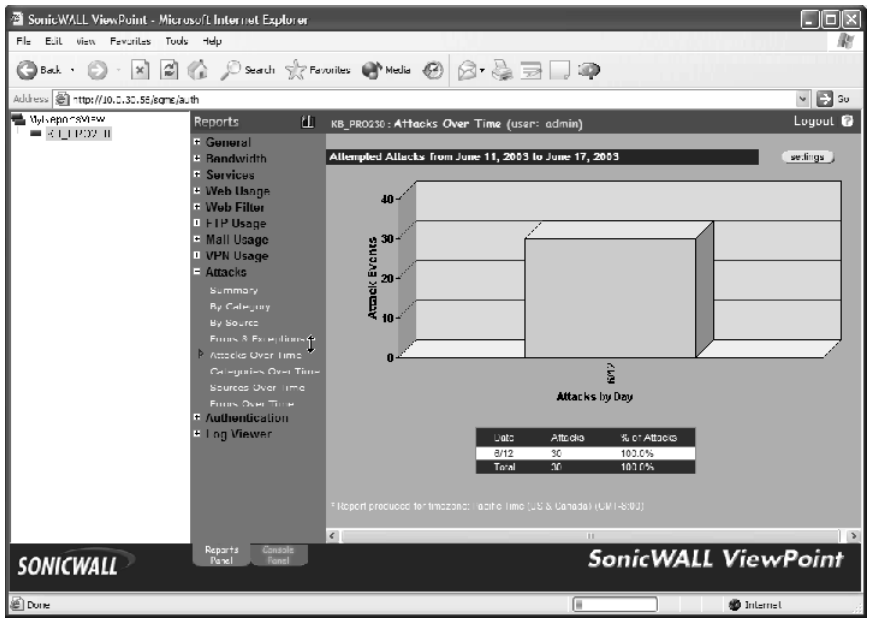
Viewing Attack Reports Over Time

The Attacks Over Time report displays the daily number of attempted attacks during the specified time period.

To view the Attacks Over Time report, follow these steps:

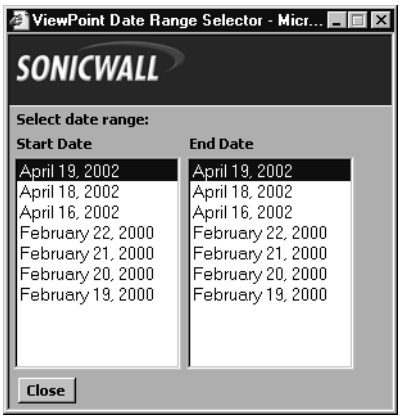
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the Attacks tree and click **Attacks Over Time**. The Attacks Over Time page opens.



5. The bar graph displays the number of attacks attempted each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of attacks on this day, compared to the time period. For example, if 10,000 attacks occurred during the time period and 1,000 attacks occurred on Thursday, its **% of Attacks** field displays 10%.

7. To change the date range of the report, click **Settings**. The ViewPoint Date Range Selector dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

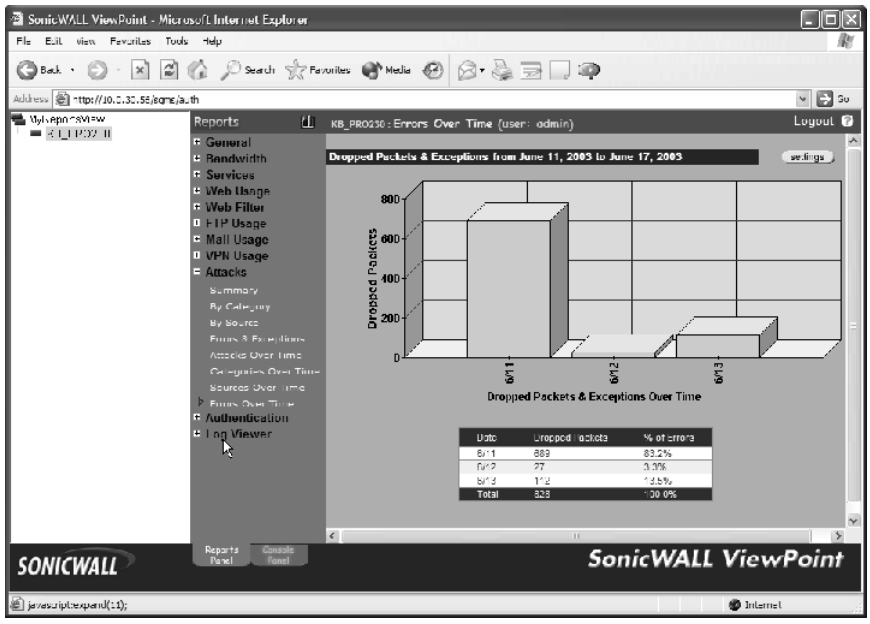
Viewing Errors Over Time

The Errors Over Time report displays the number of errors during the specified time period.

To view the Errors Over Time report, follow these steps:

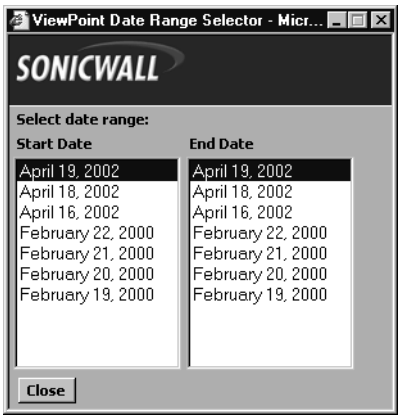
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the Attacks tree and click **Errors Over Time**. The Errors Over Time page opens.



5. The bar graph displays the number of packets that were dropped during each day of the specified time period.
6. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Dropped Packets**—number of dropped packets.
   - **% of Errors**—percentage of dropped packets on this day, compared to the time period. For example, if 10,000 packets were dropped during the time period and 1,000 packets were dropped on Wednesday, its **% of Attacks** field displays 10%.

7. To change the date range of the report, click **Settings**. The ViewPoint Date Range Selector dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

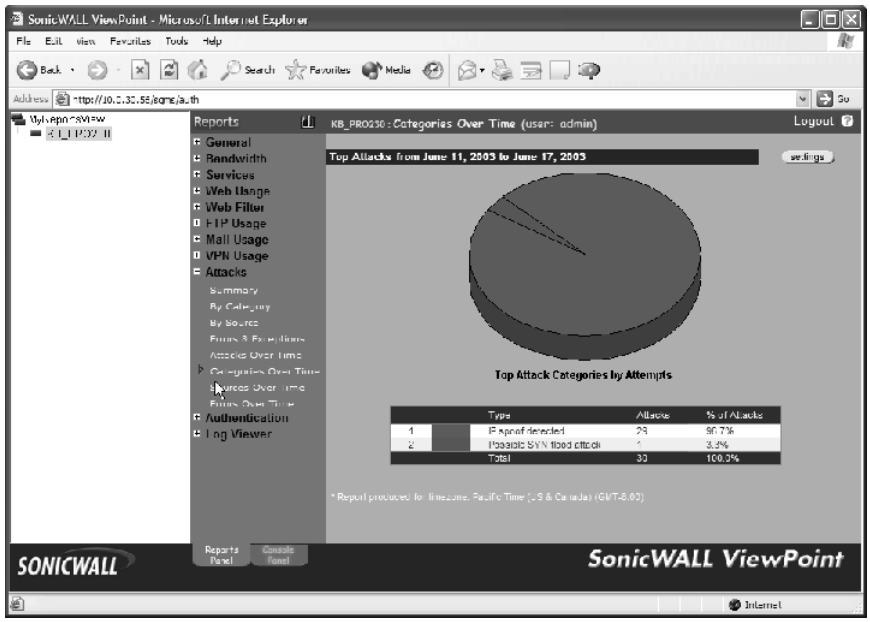
Categories Over Time

The Categories Over Time report displays the number of attacks in each attack category during the specified time period.

To view the Categories Over Time report, follow these steps:

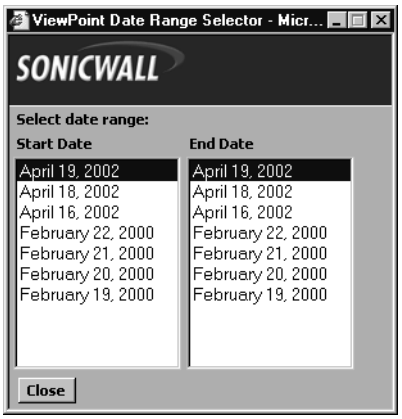
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the Attacks tree and click **Categories Over Time**. The Categories Over Time page opens.



5. The bar graph displays the number of attacks attempted each day of the specified time period.
6. The table contains the following information:
   - **Category**—category of the attack.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of attacks for this category, compared to other categories. For example, if 5,000 attacks occurred during the time period and 1,000 attacks occurred for a category, its **% of Attacks** field displays 20%.

7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings reset to the default values embedded in the software.*

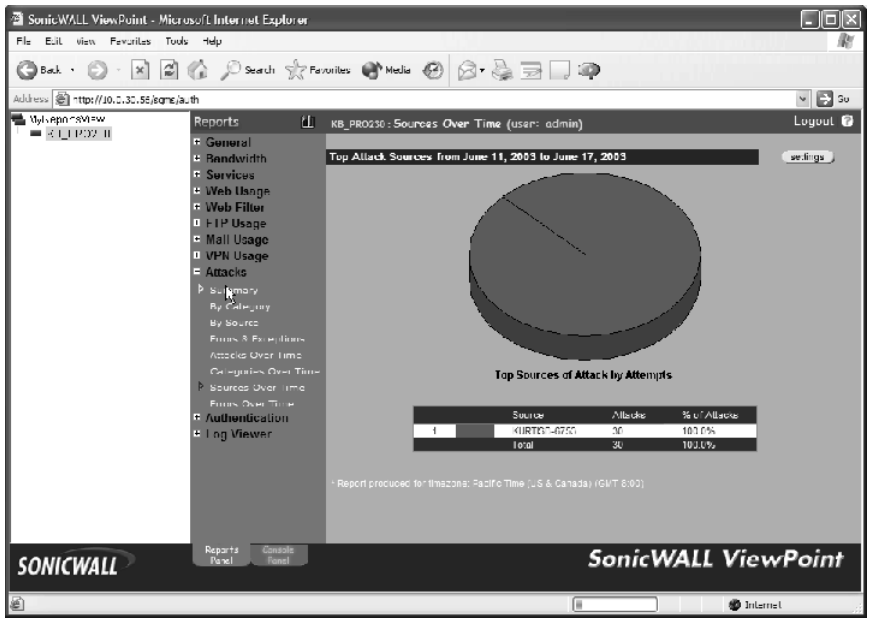
Sources Over Time

The Source Over Time report displays the number of attacks from each major source during the specified time period.

To view the Sources Over Time report, follow these steps:

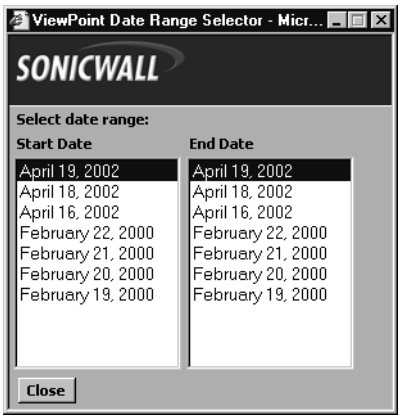
1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select the global icon, a group, or a SonicWALL appliance.

4. Expand the **Attacks** tree and click **Sources Over Time**. The Categories Over Time page opens.



5. The bar graph displays the number of attacks attempted each day of the specified time period.
6. The table contains the following information:
   - **Source**—source of the attack.
   - **Attacks**—number of attacks.
   - **% of Attacks**—percentage of attacks from this source, compared to other sources. For example, if 2,000 attacks occurred during the time period and 1,000 attacks occurred from a source, its **% of Attacks** field displays 50%.

7. To change the date range of the report, click **Settings**. The ViewPointDate Range Selector dialog box opens.



8. Select the starting and ending dates to view.
9. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected date range.

   Note: *These settings stay in effect for all reports during your active login session. Once you log out, the settings will be reset to the default values embedded in the software.*

Viewing Authentication Reports

The login reports show user logins, administrator logins, and failed login attempts for users and administrators.

Note: *The single firewall report opens in the firewall's local time. The aggregate multi-firewall report opens in Universal Time, Coordinated (UTC) or Greenwich Mean Time (GMT).*

Select from the following:

- To view user logins, see “Viewing the User Login Report” on page 144.
- To view administrator logins, see “Viewing the Administrator Login Report” on page 146.
- To view failed login attempts, see “Viewing the Failed Login Report” on page 147.

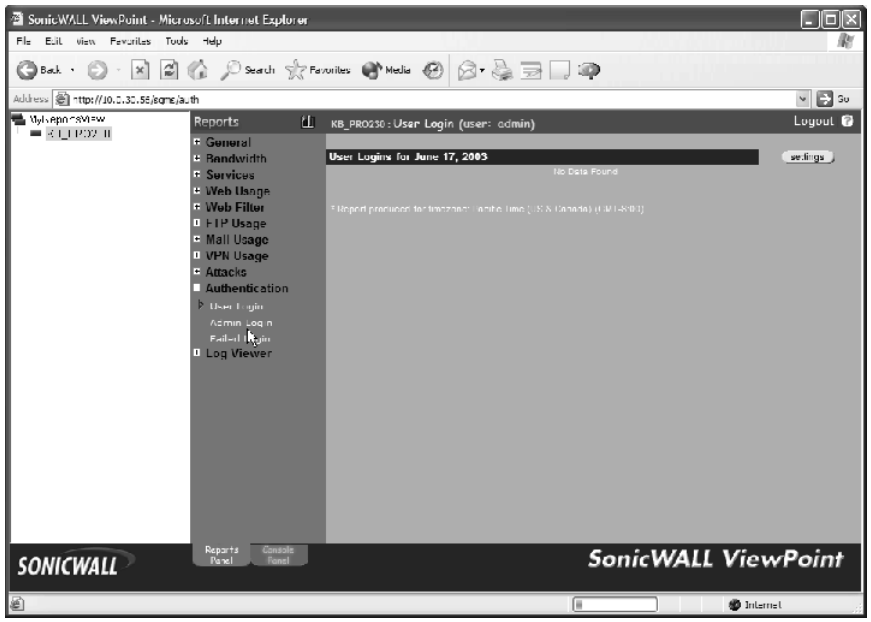
Viewing the User Login Report

The user login report shows users that logged on to the SonicWALL appliance during the specified day to bypass content filtering or to remotely access local network resources.

To view the User Login report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.

3. Select a SonicWALL appliance.
4. Expand the **Authentication** tree and click **User Login**. The User Login page opens.



5. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
6. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

7. Select the year, month, and day to view.

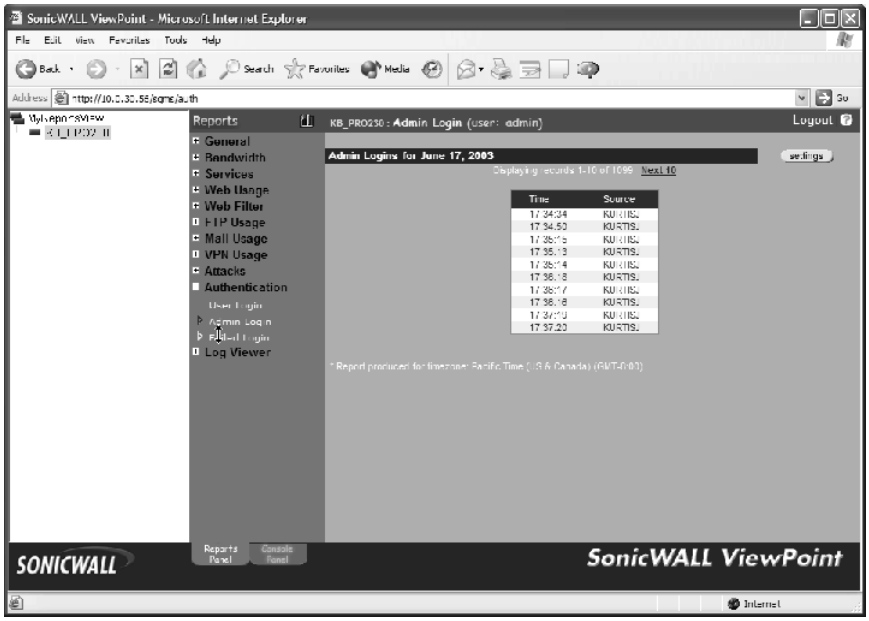
8. When you are finished, click **Close.** SonicWALL ViewPoint displays the report for the selected day.

Viewing the Administrator Login Report

The administrator login report shows successful administrator logins during the specified day. This report is useful for identifying misuse and unauthorized management of a SonicWALL appliance.

To view the Admin Login report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the **Authentication** tree and click **Admin Login**. The Admin Login page opens.



5. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
6. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

7. Select the year, month, and day to view.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

8. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

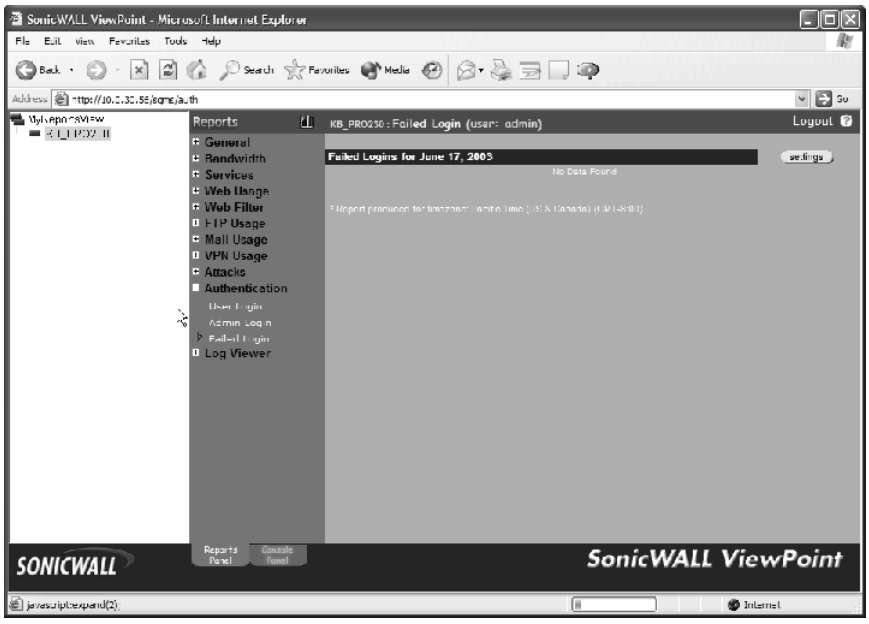
Viewing the Failed Login Report

The failed login reports shows failed login attempts for users and administrators that attempted to log on to the
SonicWALL appliance during the specified day. This report is useful for identifying unauthorized access attempts and potentially malicious activity.

To view the Failed Login report, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.

4. Expand the **Authentication** tree and click **Failed Login**. The Failed Login page opens.



5. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
   - **IP Address**—IP address of the user.
6. SonicWALL ViewPoint shows today's report. To change the date of the report, click **Settings**. The ViewPoint Settings dialog box opens.

ViewPoint Settings - Mi...
SONICWALL
June
2003
Sun Mon Tue Wed Thu Fri Sat
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
Close

7. Select the year, month, and day to view.

8. When you are finished, click **Close. SonicWALL ViewPoint** displays the report for the selected day.

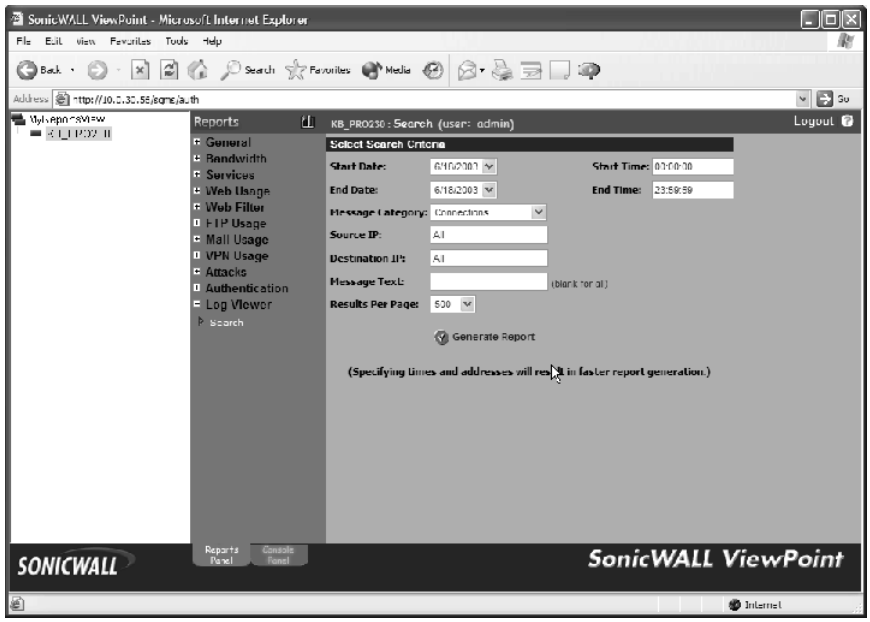
Viewing the Log

The Log Viewer contains detailed information on each transaction that occurred on the SonicWALL appliance or Ravlin device. This information is stored for the time that you specified in the configuration settings.

Note: *The Log Viewer displays raw log information for every connection. Depending on the amount of traffic, this can quickly consume a large amount of space in the database. It is highly recommended to be careful when choosing the number of days of information that is stored. For more information, see "Summarizer Settings" on page 41.*

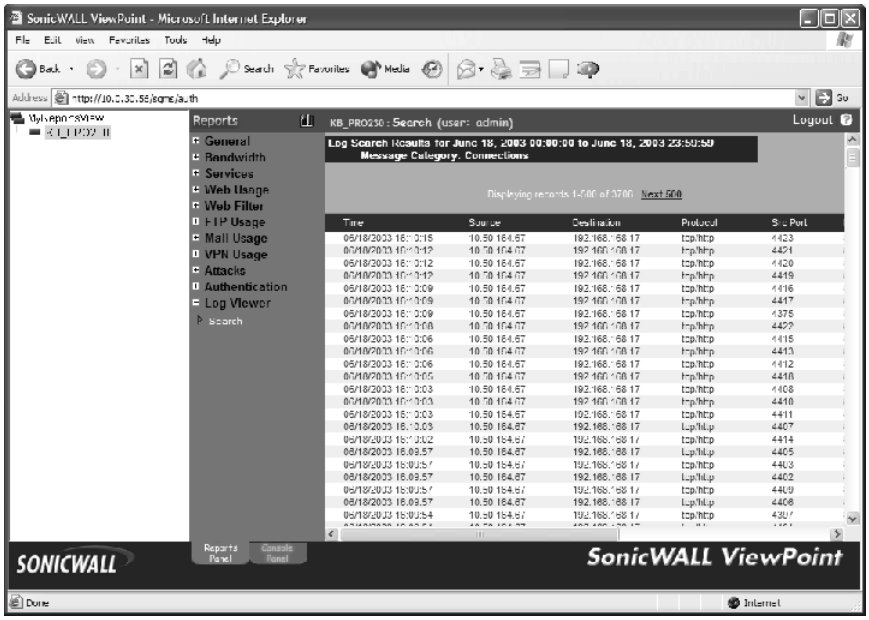
To view the log for a SonicWALL appliance, follow these steps:

1. Start and log into SonicWALL ViewPoint.
2. Click the **Reports** tab.
3. Select a SonicWALL appliance.
4. Expand the **Log Viewer** tree and click **Search**. The Search page opens.



5. Select the date to view from the **Date** list box.
6. Enter the starting time of events to view in the **Start Time** field.
7. Enter the ending time of events to view in the **End Time** field.

8. Select the type of events to view from the **Message Category** list box.
9. Enter the source IP address to view in the **Source IP Address** field. To view all IP addresses, enter All.
10. Enter the destination IP address to view in the **Destination IP Address** field. To view all IP addresses, enter All.
11. Select the number of entries to display per page from the **Results Per Page** field.
12. Click **Generate Report**. The Log Viewer Results page opens.



13. Search through the entries to find the information for which you are searching. To view the next page of entries, click **Next**.
14. To generate another report, click **Search** again in the Log Viewer Tree.

APPENDIX A

Technical Tips and Troubleshooting

Technical Tips

This section describes technical tips for operating SonicWALL ViewPoint.

Viewing the ViewPoint Database Port Number

The ViewPoint MSDE database listens at a specific port number. To determine which port is used, enter the command SVRNETCN at the command-line prompt.

This command opens the SQL Server Network Utility menu. If there are multiple SQL Server instances running on the system, you may see multiple entries in the **Instance(s) on this server** list box. To view the port, right-click **ServerName\SNWL** and select **Properties**.

Changing the ViewPoint Web Server Port Number

During installation, you specified a port number (e.g., 80) for the ViewPoint Web server. To change it after installation, follow these steps:

1. Open the following file:

   <*viewpoint_directory*>:/Tomcat/conf/server.xml

2. Locate the following line:

   ```
   Parameter name="port" value="80"
   ```

3. Change the value to another port number.
4. Save the file and exit.
5. Restart the SonicWALL ViewPoint Web server.

Changing the ViewPoint Server IP Address

If you changed the IP address of the SonicWALL ViewPoint server, follow these steps:

1. Stop all SonicWALL ViewPoint services.
2. Execute the following SQL commands from a DOS window:

   ```
   osql -U < userid > -P < password > -S 127.0.0.1\SNWL -Q "update
   sgmsdb.dbo.schedulers set ipAddress = 'new ip' where ipAddress =
   'old ip'"
   ```

   where <*userid*> is the database name “sa” and <*password*> is the database password.
3. Restart all SonicWALL ViewPoint services.

Changing the Default Syslog Server Port Number

By default, the SonicWALL ViewPoint syslog server default port number is 514 on a Windows system. To change the port, follow these steps:

1. Open the `c:\sgmsConfig.xml` file with a text editor.
2. Find and update the following line:

   `Parameter name="syslog.syslogServerPort" value="`*`port_number`*`"`

   where *port_number* is the new port number.
3. Save the file and exit.
4. Be sure the port number for the syslog server is also changed to this new value on the Log Settings, Automation, or ViewPoint page of the SonicWALL appliance.

The SonicWALL ViewPoint Log Files

SonicWALL ViewPoint provides a number of log files that can be used for troubleshooting. These files are located in the SonicWALL ViewPoint Logs directory and include the following:

- msde.log—MSDE Installation database log
- phase1upgrade.log—Phase 1 Upgrade log
- phase2install.log—Phase 2 Installation log
- phase2upgrade.log—Phase 2 Upgrade log
- schedulerDbg.txt—Syslog in debug mode
- schedulerLog.txt—Syslog in debug mode
- VPWebServerLog.txt—Web server log
- tomcaterr.log—Tomcat log
- tomcatout.log—Tomcat log
- vpSummarizerDbg.txt—Summarizer log in debug mode
- vpSummarizerLog.txt—Summarizer log in non-debug mode
- vpschedulerDbg.txt—Syslogd log in debug mode
- vpschedulerLog.txt—Syslogd log in non-debug mode

The following log files are also available:

- <viewpoint_directory>\SonicWALL_ViewPoint_2.5_installLog.log—Phase 1 Installation log
- C:\ViewPoint25_uninstall.log—Uninstall log

Encrypting the sgmsConfig.xml File

The sgmsConfig.xml and web.xml files contain encrypted data. The following information is encrypted using Tiny Encryption technology:

- Database Password
- Database Name
- Database Username
- Database Owner

To encrypt text for use in the sgmsConfig.xml and web.xml files, do the following:

1. Navigate to the <*viewpoint_directory*>:\bin folder.
2. Enter the following command at the command-line prompt:

   `java -cp . TEAV` ***`text`***

   where *text* is the text string to encrypt.

   The encrypted string is returned.
3. Add the encrypted string to the sgmsConfig.xml or web.xml file.

Note: *This procedure only performs encryption.*

Resetting the Admin Password

To reset the admin user's password to the default value of 'password', enter the following from the command-line prompt:

```
osql -U DBuser -P DBpassword -S 127.0.0.1\SNWL -Q "exit(update
sgmsdb.dbo.users set password ='5f4dcc3b5aa765d61d8327deb882cf99'
where id like 'admin')"
```

where *DBuser* is the database username “sa” and *DBpassword* is the database password.

Copying and Pasting into the ViewPoint User Interface

The Java Plug-in does not allow applets to access user clipboards. To circumvent this, you must explicitly allow applets to access your clipboard.

To do this for **ViewPoint v2.5**, follow these steps:

1. Open the **java.policy** file with a text editor. This file is usually located in the following directory:

   c:\Program Files\Java\j2rel.4.1_xx\lib\security

2. Add the following line to the top of the file after the "// "standard" properties that can be read by anyone":

   ```
   permission java.awt.AWTPermission "accessClipboard", "write";
   ```

3. Save the java.policy file and exit.
4. Restart the ViewPoint web server.

To do this for ViewPoint v2.5, follow these steps:

1. Open the **java.policy** file with a text editor. This file is usually located in the following directory:

   c:\Program Files\JavaSoft\JRE\1.3.1._xx\lib\security

2. Add the following line to the top of the file after the "// "standard" properties that can be read by anyone":

   ```
   permission java.awt.AWTPermission "accessClipboard", "write";
   ```

3. Save the java.policy file and exit.
4. Restart the ViewPoint web server.

Configuring Secure (HTTPS) Access to the ViewPoint Web Server

This section explains how to configure secure access (HTTPS) to the ViewPoint web server. To configure ViewPoint to use HTTPS, you must create a keystore with a valid test certificate.

To create a keystore for this type of installation:

For ViewPoint v2.5 that installs and uses Tomcat v4.1.24 to create a keystore, follow these steps:

follow these steps:

1. Stop the SGMS Web Server service.
2. From the command-line on the SonicWALL ViewPoint server, change to the following directory:

   ```
   viewpoint_directory\jre\bin
   ```

   where viewpoint_directory is the directory where SonicWALL ViewPoint is installed.

3. Enter the following command:

   ```
   .\keytool -genkey -alias spcert -keyalg RSA -keystore
   viewpoint_directory\etc\keystore
   ```

4. You are prompted to enter the keystore password and other information.
5. When prompted to confirm the information, type yes and press Enter.
6. Enter key password for <spcert>. If the password is the same as the keystore password, hit Enter.

The certificate is issued for evaluation and testing purposes. To create a secure website using this certificate, see “Creating a Secure Website” section below. To use HTTPS with a valid certificate, you will need to obtain a certificate through a valid certificate authority (e.g., Verisign and Thawte) and store the certificate in the keystore that you just created.

Note: *Note: For information on getting a certificate from Thawte, visit http://www.orionserver.com/docs/sslhowto.html.*

Creating a Secure Website

This section describes how to create a secure website with server side authentication. To do this, follow these steps:

1. Open the <viewpoint_directory>\Tomcat\conf\server.xml file with a text editor.
2. Locate the following entry:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!--
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8443" minProcessors="5" maxProcessors="75"
enableLookups="false"
acceptCount="100" debug="0" scheme="https" secure="true"
useURIValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFac-
tory"
clientAuth="false" protocol="TLS" />
</Connector>
-->
```

3. Remove the comment characters (<!--, -->).
4. Change the port value from 8443 to 443.
5. Enter the following lines below the Factory entry:

   ```
   keystoreFile="viewpoint_directory\etc\keystore" keystore-
   Pass="keystore_password"
   ```

   where keystore_password is the keystore password that you entered when creating the certificate and viewpoint_directory is the directory where SonicWALL ViewPoint is installed.

The following is an example of a modified server.xml entry:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 443 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="443" minProcessors="5" maxProcessors="75"
enableLookups="false"
acceptCount="100" debug="0" scheme="https" secure="true"
useURIValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFac-
tory"
keystoreFile="sgms_directory\etc\keystore" keystore-
Pass="keystore_password"
clientAuth="false" protocol="TLS" />
```

```
</Connector>
```

6. To disallow normal HTTP traffic, locate and comment out the following section:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8080 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="80" minProcessors="5" maxProcessors="75"
enableLookups="false" redirectPort="8443"
acceptCount="100" debug="0" connectionTimeout="20000"
useURIValidationHack="false" disableUploadTimeout="true" />
```

Note: *If the SNWL ViewPoint WebServer is not installed on port 80, replace the port number with the one assigned to the SNWL ViewPoint WebServer on your ViewPoint 2.5 system.*

7. When you are finished, it should look like the following:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8080 -->
<!--
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="80" minProcessors="5" maxProcessors="75"
enableLookups="false" redirectPort="8443"
acceptCount="100" debug="0" connectionTimeout="20000"
useURIValidationHack="false" disableUploadTimeout="true" />
-->
```

8. Save the file and exit.
9. Restart the SNWL ViewPoint WebServer service.

Securely Accessing SonicWALL ViewPoint

To securely access SonicWALL ViewPoint, open a web browser and enter https://viewpoint_address where viewpoint_address is the address of the SonicWALL ViewPoint server. If you are using a Windows server, modify the desktop shortcut. Make sure it points to https://localhost.

To create a keystore for this type of installation:

ViewPoint v2.5 Using Tomcat v4.1.24,

follow these steps:

1. Stop the SNWL ViewPoint Webserver service.
2. From the command-line on the SonicWALL ViewPoint server, change to the following directory:

   \jre\bin

   within the directory where SonicWALL ViewPoint is installed.

3. Enter the following command:

   .\keytool -genkey -alias spcert -keyalg RSA -keystore viewpoint_directory\etc\keystore

4. You are prompted to enter the keystore password and other information.
5. When prompted to confirm the information, type yes and press Enter.
6. Enter key password for ????. If the password is the same as the keystore password, hit Enter.

The certificate is issued for evaluation and testing purposes. To create a secure website using this certificate, see “Creating a Secure Website” on page 157. To use HTTPS with a permanent certificate, you will need to obtain a certificate through a valid certificate authority (e.g., Verisign and Thawte) and store the certificate in the keystore that you just created.

Creating a Secure Website

This section describes how to create a secure website with server side authentication. To do this, follow these steps:

1. Open the <*viewpoint_directory*>\jre\lib\security\java.security file with a text editor.
2. Locate the following entry:

   ```
   provider.2
   ```

3. Replace it with the following:

   ```
   provider.3
   ```

4. Insert the following line above the line that you just edited:

   ```
   security.provider.2=com.sun.net.ssl.internal.ssl.Provider
   ```

5. Save the file and exit.
6. Open the <*viewpoint_directory*>\Tomcat\conf\server.xml file with a text editor.
7. Locate the following entry:

   ```
   <!--
   <Connector className="org.apache.tomcat.service.PoolTcpConnector">
   <Parameter name="handler"
   value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
   <Parameter name="port"
   value="8443"/>
   <Parameter name="socketFactory"
   value="org.apache.tomcat.net.SSLSocketFactory" />
   </Connector>
   -->
   ```

8. Remove the comment characters (<!--, -->).
9. Change the port value from 8443 to 443.
10. . Enter the following lines below the port entry:

```
<Parameter name="keypass" value="keystore_password"/>
<Parameter name="keystore" value="viewpoint_directory\etc\keystore"/>
<Parameter name="clientAuth" value="false"/>
```

where *keystore_password* is the keystore password that you entered when creating the certificate and *viewpoint_directory* is the directory where SonicWALL ViewPoint was installed.

The following is an example of a modified server.xml entry:

```
<Connector className="org.apache.tomcat.service.PoolTcpConnector">
<Parameter name="handler"
value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
<Parameter name="port"
value="443"/>
<Parameter name="keypass" value="sgms11"/>
<Parameter name="keystore" value="D:\SGMS2\etc\keystore"/>
<Parameter name="clientAuth" value="false"/>
<Parameter name="socketFactory"
value="org.apache.tomcat.net.SSLSocketFactory" />
</Connector>
```

11. To disallow normal HTTP traffic, locate and comment out the following section:

```
<!-- Normal HTTP -->
<Connector className="org.apache.tomcat.service.PoolTcpConnector">
<Parameter name="handler"
value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
<Parameter name="port" value="80"/>
</Connector>
```

When you are finished, it should look like the following:

```
<!-- Normal HTTP -->
<!--
<Connector className="org.apache.tomcat.service.PoolTcpConnector">
<Parameter name="handler"
value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
<Parameter name="port" value="80"/>
</Connector>
-->
```

12. Save the file and exit.
13. Restart the ViewPoint Web Server service.

Securely Accessing SonicWALL ViewPoint

To securely access SonicWALL ViewPoint, open a web browser and enter `https://viewpoint_ipaddress` where viewpoint_address is the address of the SonicWALL ViewPoint server.

Modify the desktop shortcut and make sure it points to `https://localhost`.

Troubleshooting

This section describes troubleshooting information for SonicWALL ViewPoint.

Installation Failure

Problem:

ViewPoint 2.0 installation might fail if it cannot connect to the MSDE database on a Windows 2000 system. This can happen if you are installing ViewPoint 2.0 on a Windows system that is not connected to the network.

Solution:

To recover from this problem, follow these steps:

1. Uninstall ViewPoint 2.0.
2. Ensure your Windows system is on the network.
3. Ensure that the hostname for your PC is 20 characters or less.
4. Open the following file with a text editor:

   `c:\winnt\system32\drivers\etc\hosts`
5. Add the following entries for 127.0.0.1 (after the existing localhost entry):

   127.0.0.1 localhost

   127.0.0.1 *myMachineName*

   Where *myMachineName* is the name of your Windows system

   Note: *To obtain the hostname of your system, enter the command "hostname" at the command-line prompt.*
6. Reboot your Windows system and run <*viewpoint_directory*>\bin\postinstall.bat from the DOS prompt.
7. Reboot your Windows system.

If the above does not work, perform the following steps:

1. At the DOS prompt, from the <*viewpoint_directory*>\bin folder, run the following SQL command:

   osql -U *username* -P *password* -S 127.0.0.1\SNWL

   where *username* is the database name 'sa' and *password* is the database password
2. At the database prompt (>), enter the following commands:

   > select @@servername

```
> go
```

This returns the ViewPoint servername from the database in this format servername\SNWL. Record the servername (without the \SNWL).

3. Exit from the database by entering the following:

```
> quit
```

4. From the DOS prompt, enter the command SVRNETCN. The SQL Server Network Utility opens.
5. If there are multiple SQL Server instances running on the system, you may see multiple entries in the **Instance(s) on this server** list box. To view the port, right-click **ServerName\SNWL** and select Properties.
6. Write down the port number.
7. Edit the C:\sgmsConfig.XML file and look for the following line:

   <Parameter name="dburl" value="jdbc:inetdae7a:127.0.0.1/SNWL"/>

8. Replace the value of 127.0.0.1\SNWL with the following:

```
servername:port number
```

9. Save and exit from the sgmsConfig.XML file.
10. At the DOS prompt, from the <*viewpoint_directory*>\bin folder, run the postinstall.bat file.
11. Reboot your Windows system.

Viewpoint Cannot Install SQLAgent Service on Windows 2000

Problem:

When the ViewPoint installer attempts to install MSDE 2000 on a Windows 2000 Server Domain Controller, the progress bar rolls back at the end and the setup fails. The following conditions must be true for this to occur:

- The server on which MSDE is being installed is not the first Domain Controller in the domain.
- The Primary (or first) Domain Controller is not available.

With verbose logging enabled (i.e, setup.exe /L*v c:\temp\msde.log), you will see the following error in the setup log:

```
Starting custom action InstallSQLAgentSecurity
InstallSQLAgentSecurity failed (MYSERVER,LocalSystem,87).
Action ended 13:58:26: InstallFinalize. Return value 3.
```

Solution:

To correct this problem, make certain that:

- The Primary Domain Controller (PDC) is available when installing MSDE 2000 on a Backup Domain Controller.
- You are logged into the Windows system as an Administrator with full Administrator access rights.

ViewPoint Cannot Connect to the MSDE Database on a Windows 2000 System

Problem:

The PC on which ViewPoint is being installed is not on the network.

Solution:

To recover from this, do the following:

1. Uninstall ViewPoint

2. Ensure your Windows system is on the network

3. In the hosts file, typically located at:

```
c:\winnt\system32\drivers\etc\hosts
```

add an entry for 127.0.0.1 (after the existing localhost entry):

```
127.0.0.1 localhost
127.0.0.1 myMachineName
```

where, myMachineName is the name of your Windows system (you can obtain the hostname by typing the command "hostname" at the DOS prompt).

4. Reboot your Windows system, and install ViewPoint.

ViewPoint Cannot Locate the MSDE Database

Problem:

SonicWALL ViewPoint 2.0 installation fails at Phase 2, not finding the MSDE database with the Upgrade Failed message:

[DBNETLIB]SQL Server does not exist or access denied. [DBNETLIB]ConnectionOpen (Connect()).

Java doesn't recognize the MSDE database using the URL "127.0.0.1\SNWL". This is an issue on some Windows 2000 servers.

Solution:

Perform the following steps to continue with the installation:

1. Exit from the Phase 2 Install by clicking "Cancel".

2. Open a DOS window and run the SQL Server Network Utility—SVRNETCN.EXE. Typically, this program is located in the C:\Program Files\Microsoft SQL Server\80\Tools\Binn folder.

3. If there are multiple SQL Server instances running on the system, you may see multiple entries in the ‘Instance(s) on this server" list box. Select the item ServerName\SNWL from the list box.

4. Select TCP/IP from the Protocols list and click Properties.

5. Write down the port number.

6. Exit from the menu.

7. Make the following modifications to the c:\sgmsConfig.xml and <viewpoint_directory>\Tomcat\webapps\sgms\WEB-INF\web.xml files:

```
Change the dbURL value from "127.0.0.1/SNWL" to "localhost:portnumber"

Change the dbhost value "127.0.0.1\SNWL" to "127.0.0.1"
```

8. Make the following modifications to <viewpoint_directory>\SQL\bldMSDB.bat:

```
Change the value for User to sa

Change the value for Password to
<yourdatabasepasswordselectedatphase1>
```

9. Open a DOS window and from the <viewpoint_directory>\SQL folder, run the bldMSDB.bat program to install the MSDE database.

10. Navigate to <viewpoint_directory>\Temp and run the following programs to install the SNWL ViewPoint Summarizer and SNWL ViewPoint Syslogd services:

```
schedInstall.bat

vpInstall.bat
```

11. Navigate to <viewpoint_directory>\Tomcat\bin and run the following program to install the SNWL ViewPoint WebServer service:

```
tomcat.bat install
```

12. Reboot your Windows system.

ViewPoint Cannot Install Due to an Unexpected Signal Error

Problem:

Installation of SonicWALL ViewPoint fails on a system with the exception error: An unexpected exception has been detected in native code outside the VM. Unexpected Signal. This is a Java related issue that occurs because the Windows system has multiple monitors set to different color depths.

Solution:

Ensure that all monitors are set to the same color depth. Under these conditions, the ViewPoint installation will succeed. After ViewPoint is installed, set the display systems back to their original color depth settings. Changing these settings has no further affect on ViewPoint performance or operations.

APPENDIX B

ViewPoint Reports

The following table lists the type of Reports that can be generated and viewed while logged into the ViewPoint. The table also indicates whether the report is available at the Unit or Group level.

Report Name	Unit level	Group Level
Bandwidth		
Summary	Yes	Yes
Monitor	Yes	
Top Users	Yes	
Over Time	Yes	Yes
Top Users Over Time	Yes	
Services		
Summary	Yes	
Monitor	Yes	
Web Usage		
Summary	Yes	Yes
Top Sites	Yes	
Top Users	Yes	
By User	Yes	
Over Time	Yes	Yes
Top Sites Over Time	Yes	
Top Users Over Time	Yes	
By Users Over Time	Yes	
Web Filter Usage		
Summary	Yes	Yes
Top Sites	Yes	
Top Users	Yes	
By User	Yes	
Over Time	Yes	Yes
Top Sites Over Time	Yes	

Top Users Over Time	Yes	
By Users Over Time	Yes	
FTP Usage		
Summary	Yes	Yes
Top Users	Yes	
Over Time	Yes	Yes
Top Users Over Time	Yes	
Mail Usage		
Summary	Yes	Yes
Top Users	Yes	
Over Time	Yes	Yes
Top Users Over Time	Yes	
VPN Usage		
Summary	Yes	Yes
Top Users	Yes	
Over Time	Yes	Yes
Top Users Over Time	Yes	
Attacks		
Summary	Yes	Yes
By Category	Yes	
By Source	Yes	
Errors & Exceptions	Yes	Yes
Attacks Over Time	Yes	Yes
Categories Over Time	Yes	
Sources Over Time	Yes	
Errors Over Time	Yes	Yes
Authentication		
User Login	Yes	
Admin Login	Yes	
Failed Login	Yes	